APPLICATIONS OF RAPIDLY MIXING MARKOV CHAINS TO PROBLEMS IN GRAPH THEORY

DISSERTATION

Presented to the Graduate Council of the
University of North Texas in Partial
Fulfillment of the Requirements

For the Degree of

DOCTOR OF PHILOSOPHY

By

Dayton C. Simmons, III, B.S., M.S.

Denton, Texas

August, 1993

APPLICATIONS OF RAPIDLY MIXING MARKOV CHAINS TO PROBLEMS IN GRAPH THEORY

DISSERTATION

Presented to the Graduate Council of the
University of North Texas in Partial
Fulfillment of the Requirements

For the Degree of

DOCTOR OF PHILOSOPHY

By

Dayton C. Simmons, III, B.S., M.S.

Denton, Texas

August, 1993

NB

Simmons, III, Dayton C., Applications of Rapidly Mixing Markov Chains to Problems in Graph Theory, Doctor of Philososphy (Mathematics), August, 1993, 72 pp., bibliography, 55 titles.

In this dissertation the results of Jerrum and Sinclair on the conductance of Markov chains are used to prove that almost all generalized Steinhaus graphs are rapidly mixing and an algorithm for the uniform generation of $2-(4k+1,4,1)$ cyclic Mendelsohn designs is developed.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

Given a population of objects characterized by some property, the first task a combinatorialist might undertake is to determine its cardinality. In many cases this is a difficult task, and an approximate answer would suffice. Another task confronting our combinatorialist might be to choose (or generate) an object uniformly at random from the population. Again, in many cases this can be a daunting task, and an object chosen almost uniformly would be sufficient. These two seemingly disparate problems have been shown to be equivalent for sets defined by self reducible relations [Va]. Thus one need only consider the problem of uniform generation.

One powerful tool in tackling the problem of almost uniform generation is the Markov chain technique. In the Markov chain technique, one first attempts to construct a Markov chain whose states are the structures of interest and whose stationary distribution is uniform on the state space. If such a chain can be constructed, one then simulates the chain until its distribution is close to stationarity. The state of the chain after this mixing will be an element of our set with almost uniform distribution.

However, for the Markov chain technique to be useful we need to meet several criteria. Firstly, we want the steps of the chain to be efficiently simulated. Secondly, we require that the chain converge rapidly to its stationary distribution, that is, be rapidly mixing. Now, the task of constructing a chain whose steps are efficiently simulated generally poses no problem; however, determining rate of convergence can be a much more difficult undertaking.

The recent work of Jerrum and Sinclair provides a tool for addressing just this question. In [SiJe], they show that the mixing rate of a Markov chain can be analyzed by examining the underlying digraph of the chain. Thus in Chapter 2, we present classic results in Markov chain theory and the results of Jerrum and Sinclair.

An important application of probability to mathematics occurs in the theory of random graphs. One of the basic questions in random graph theory is to determine the asymptotic proportion of graphs possessing a given property. If this number is one, then almost all graphs are said to possess the property. An interesting class of graphs about which much is known is the class of generalized Steinhaus graphs [BrMo]. In Chapter 3, we define Steinhaus graphs and generalized Steinhaus graphs, present the results of Brand and other authors, and prove that almost all generalized Steinhaus graphs are rapidly mixing.

Finally, in Chapter 4 we lay the foundations of an algorithm for the uniform generation of cyclic Mendelsohn designs. First, we define Mendelsohn designs and their equivalent formulation as difference families. Then we construct a chain whose states are difference families and where the transistions between states can be easily simulated. We then obtain upper and lower bounds on the degrees of vertices of the underlying digraph of this chain.

CHAPTER II

MARKOV CHAINS AND RANDOM WALKS

1. Introduction

In this chapter we present both classical and recent results in the theory of Markov chains. In Section 2, we give definitions and basic theory culminating in the fact that a finite-state, homogeneous, irreducible, aperiodic Markov chain has a unique stationary distribution, and in Section 3 we note the equivalence of simulating a Markov chain and taking a random walk on a graph. Then we discuss recent results of Mark Jerrum and Alistair Sinclair on applications of Markov chains. In Section 4, we discuss how Markov chains may be implemented to approximate the size of a population of combinatorial objects and to generate examples almost uniformly at random. The efficacy of such algorithms, as pointed out by Jerrum and Sinclair, depend on the rapid convergence of a Markov chain to stationarity. Such chains are said to be rapidly mixing. In Section 5, we give a powerful criterion discovered by Sinclair for analyzing the mixing rate of Markov chains.

There are many excellent references on the theory of Markov chains. In particular [Bil], [Fe], [GrSt],[Ro1] and [Ro2] are quite good. The following text borrows heavily from all of the above sources. Our usage attempts to be consistent where possible with [Bil], [GrSt] and [Ro2].

2. Preliminaries

The theory of stochastic processes is the branch of probability that addresses systems that evolve or change. Specifically, a *stochastic process* is an indexed collection of random variables, $\{X_t : t \in T\}$, defined on a probability space $(\Omega, \mathcal{F}, P)$. One usually thinks of the index set T, which may be continuous or discrete, as representing time. In this section we consider a special class of stochastic processes, Markov chains.

Let S be a countable set and let $X = \{X_t : t \in T\}$ be a stochastic process such that $X_t(\Omega) \subseteq S$ for all t. The set S is referred to as the *state* or *phase space* and if $X_n = i$ we say that X_n is in state i at time n. If S is finite, X is said to be of *finite-state* and, in this case, we may and will consider $S = \{1, 2, \cdots, |S|\}$, without loss of generality.

Definition 2.2.1. ([Bil] p.107) The stochastic process X is a *discrete-time Markov chain* if

$$\Pr[X_{n+1} = j \mid X_0 = i_0, X_1 = i_1, \cdots, X_n = i_n] = \Pr[X_{n+1} = j \mid X_n = i_n] = P_{i_n j}$$

for all sequences $i_0, i_1, \cdots, i_n$ such that $\Pr[X_0 = i_0, X_1 = i_1, \cdots, X_n = i_n] \neq 0$.

This condition is known as the *Markov property* and can be interpreted as saying that "the conditional distribution of any future state X_{n+1} given the past states $X_0, X_1, \cdots, X_{n-1}$ and the present state X_n is independent of the past states and depends only on the present state."([Ro2]). The numbers $P_{i_n j}$, are the *transition* *probabilities* of the chain and represent the probability that a chain in state i at time n will make a transition to state j in one step.

In general the transition probabilities are dependent on time. If not then

$$\Pr[X_{n+1} = j \mid X_n = i] = \Pr[X_1 = j \mid X_0 = i] = P_{ij}$$

for all n, i, j and the chain is said to be *homogeneous.* In this case, we let $P = (P_{ij})$ be the matrix of the one-step transition probabilities and refer to P as the *transition matrix* of the chain. Henceforth, all of our Markov chains will be assumed to be homogeneous, discrete-time, and of finite-state.

We now consider the n-step transition probabilities, that is, the probabilities of going from one state to another in n steps. These probabilities are given by the *Chapman-Kolmogorov equations* ([GrSt p.196). In our case of a finite state space, these equations are

$$P_{ij}(n+m) = \sum_{k=1}^{|S|} P_{ik}(n)P_{kj}(m) \quad \text{for all } n, m \geq 0, \text{ all } i, j,$$

where $P_{ij}(n)$ denotes the probability of going from state i to state j in n steps.

Let P_n denote the matrix of the n-step transition probabilities. Then from the above equations we get $P_{n+m} = P_n P_m$. This property is refered to as the *semigroup property* of the chain. In particular, we have $P_n = P^n$. That is, the n-step transition probabilities can be computed by taking the n-th power of the transition matrix. Furthermore, if p_0 is any initial distribution, then the distribution of the chain after t steps, p_t, is given by $p_t = p_0 P^t$.

We now note some important properties of Markov chains necessary for our investigation.

Definition 2.2.2. ([Ro1] p.141) A state j of a Markov chain is said to be *accessible* from a state i if $P_{ij}^n > 0$ for some integer n. Two states are said to *communicate* if they are accessible from each other.

Proposition 2.2.3. *The relation of communication is an equivalence relation.*

Definition 2.2.4. Two states are said to be of the same *class* if they communicate. A Markov chain that has only one class is said to be *irreducible.*

Thus a Markov chain is irreducible if and only if any state is accessible from another.

Definition 2.2.5. ([Ro2] p.104) A state i is said to have *period* d if $P_{ii}^n = 0$ whenever n is not divisible by d and d is the greatest integer with this property. A state with period 1 is said to be *aperiodic.*

Proposition 2.2.6. ([Ro2] p.105) *Periodicity is a class property, that is, if i and j communicate then $d(i) = d(j)$.*

Let f_{ij}^n denote the probability that, starting in state i, the first transition to state j occurs at time n. That is,

$$f_{ij}^n = \Pr\left[X_n = j, X_{n-1} \neq j, X_{n-2} \neq j, \cdots, X_1 \neq j \mid X_0 = i\right].$$

Then,

$$f_{ij} = \sum_{n=1}^{\infty} f_{ij}^{n}$$

denotes the probability of ever making a transition from i to j. The f_{ij}^{n} are called the *first passage probabilities* of the chain.

Definition 2.2.7. ([Ro2] p.105) A state i is said to be *recurrent* or *persistent* if $f_{ii} = 1$, and *transient* otherwise.

Proposition 2.2.8. ([Ro2] p.106) *Recurrence is a class property. That is, if i and j communicate and i is recurrent, then j is recurrent.*

Definition 2.2.9. ([GrSt], p.203) Let $T_j = \min\{n \geq 1 : X_n = j\}$ denote the time of first passage to state j. The *mean recurrence time* μ_i of a state is defined as

$$\mu_i = \ \mathrm{E}(T_i \mid X_0 = i) = \begin{cases} \sum_n n f_{ii}^{n} & \text{if } i \text{ is persistent} \\ \infty & \text{if } i \text{ is transient.} \end{cases}$$

Recurrent states may be classified as null or non-null according as μ_i is finite.

Definition 2.2.10. ([GrSt], p.203) A recurrent state i is called $\begin{cases} \textit{null} & \text{if } \mu_i = \infty \\ \textit{non-null} & \text{if } \mu_i < \infty. \end{cases}$

Null (non-null) recurrence is a class property. The next proposition gives us a condition for the existence of non-null states.

Lemma 2.2.11. ([GrSt], p.206) *If S is finite, then at least one state is persistent and all persistent states are non-null.*

The next definition is important.

Definition 2.2.12. ([GrSt], p.203) A state is called *ergodic* if it is persistent, non-null and aperiodic.

Thus if X is an irreducible, aperiodic, finite-state Markov chain, then all states are ergodic. In the case that all states are ergodic, we say that the chain X is ergodic. Now let us consider the limiting behavior of the chain.

Definition 2.2.13. ([GrSt], p.207) The vector $\pi = \langle \pi_1, \pi_2, \cdots, \pi_{|S|} \rangle$ is called a *stationary distribution* of the chain if

(a) $\pi_j \geq 0$ for all j, and $\sum_j \pi_j = 1$

(b) $\pi = \pi P$, that is $\pi_j = \sum_i \pi_i p_{ij}$ for all j.

Theorem 2.2.14. [GrSt p.208] *An aperiodic, irreducible chain has a stationary distribution π if and only if all the states are non-null persistent; in this case, π is the unique stationary distribution and is given by $\pi_i = {\mu_i}^{-1}$ for each $i \in S$, where μ_i is the mean recurrence time of i.*

Thus any irreducible, ergodic Markov chain has a stationary distribution.

3. Connection with graphs

It is often convenient to view Markov chains in the context of graphs. Clearly, we can represent a Markov chain by a directed graph, $G = (V, E)$. Simply let $V = S$ and let $E = \{(i, j) \mid P_{ij} \neq 0\}$. In this section we will show that there is a one-to-one correspondence between transition matrices (or equivalence classes of Markov chains) and normalized, weighted, directed graphs. This is of course, a well known result in the theory of Markov chains. We will then show that the simulation of an irreducible aperiodic Markov chain is equivalent to a random walk on the underlying digraph of the chain.

Proposition 2.3.1. *There is a one-to-one correspondence between transition matrices and normalized, weighted, directed graphs.*

Proof: Let P be the transition matrix of a Markov chain. We associate with P the *underlying graph* of P, $G_P(V, W)$ as follows. Let $V = S$ and let $W = \{w_{ij} = \pi_i P_{ij} \mid i, j \in S\}$. Clearly, G_P is a weighted, directed graph. Now, summing up the edge weights,

$$\sum_i \sum_j \pi_i P_{ij} = \sum_i \pi_i \sum_j P_{ij} = \sum_i \pi_i = 1$$

we see that G_P is normalized.

Conversely, let $G(V, W)$ be a normalized, weighted, directed graph. Without loss of generality we will assume that $V = \{1, 2, \cdots, |V|\}$. For all $i, j \in V$ let $P_{ij} = \frac{w_{ij}}{\sum_l w_{il}}$. Then by the Kolmogorov Existence Theorem([Bil], p.510), there is a Markov chain X with state space $S = V$ having the transition probabilities P_{ij}. □

We can now note the analogues of some of the properties of a Markov chain X in the underlying digraph, G. In particular,

- j is accessible from i if and only if there is a path from i to j,
- i and j communicate if and only if there is a cycle containing i and j,

- X is irreducible if and only if G is connected,
- if X is irreducible, then X is aperiodic if and only if G is not bipartite.

We will now show that the simulation of a Markov chain is equivalent to a random walk on the underlying digraph of the chain. First we will examine random walks on (unweighted, undirected) graphs.

Definition 2.3.2. Let $G = (V, E)$ be an unweighted, undirected graph. A *random walk* on G is a discrete-time, homogenous Markov chain, $X_0, X_1, X_2, \cdots$, taking values in V such that

$$\Pr\left[X_{k+1} = j \mid X_k = i\right] = \begin{cases} \dfrac{1}{\deg(i)}, & \text{if } j \text{ is a neighbor of } i \\ 0, & \text{otherwise.} \end{cases}$$

Thus, to execute a random walk on a graph we start with an arbitrary vertex v_0, and choose v_1 from the neighboring vertices with probability $\frac{1}{\deg(v_0)}$. We then continue this process, choosing vertex v_k from the neighbors of v_{k-1} with probability $\frac{1}{\deg(v_{k-1})}$ for all $k > 0$.

Now suppose that $G = (V, W)$ is a normalized, weighted, directed graph with edge weights w_{ij}. As before, a random walk on G commences from an arbitrary initial vertex $i = v_0$, but instead of choosing the next vertex uniformly at random from the neighbors of v_0, we choose a neighbor j with probability $\frac{w_{ij}}{\sum_l w_{il}}$.

Now when we simulate a Markov chain, we generate a sequence of states, $s_0, s_1, s_2, \cdots$ where $P\left[s_n = j \mid s_{n-1} = i\right] = P_{ij}$. And when we execute a random walk on its underlying graph, we generate a sequence of vertices $v_0, v_1, \cdots$ where $P\left[v_n = j \mid v_{n-1} = i\right] = \frac{\pi_i P_{ij}}{\sum_l \pi_i P_{il}} = \frac{\pi_i P_{ij}}{\pi_i} = P_{ij}$. Hence, simulating of a Markov chain is equivalent to taking a random walk on its underlying digraph.

4. Applications

A problem which frequently arises in combinatorics is to count the number of instances of a certain type of combinatorial structure. Consider, for example, the problem of determining the number, T_n, of labeled trees of order n. The solution to this well-known problem is known as Cayley's formula.

Proposition 2.4.1. [Cayley] *Let T_n denote the number of labeled trees of order n. Then $T_n = n^{n-2}$.*

As E. Palmer ([Pa] p. 4) notes, the discovery of this proposition is unavoidable if one merely lists the numbers of labeled trees of order $n \leq 5$. In fact, proofs abound for Cayley's formula. J.W. Moon [Mo2] is said to have collected ten distinct proofs of this theorem and, H. Prüfer [Pr] has given a particularly elegant proof.

However, it is usually prohibitive to take such an approach to counting. After examining a few initial cases, a conjectured solution might not be forthcoming or may be difficult to prove. Also it may happen, as in the above example, that the number of structures is exponentially large in terms of the problem size. Thus generating all the possible structures for a given problem size could prove to be intractable.

Consider, for example, the open problem of computing the permanent [Br2]. Given a square 0-1 matrix $M = (m_{ij})$ of size n, the permanent of M is defined by

$$\mathrm{per}(M) = \sum_{\sigma} \prod_{1 \leq i \leq n} m_{i\sigma(i)},$$

where σ ranges over all permutations of $\{1, 2, \cdots, n\}$.

It has been observed that this problem is equivalent to counting the number of perfect matchings, or 1-factors, in the bipartite graph $G(V_1, V_2, E)$, where $|V_1| = |V_2| = n$ and $E \subset V_1 \times V_2$ such that $(i, j) \in E$ if and only if $m_{ij} = 1$.

Valiant has shown that this problem is #P-complete [JeSi2]. In such cases, it is often just as good to have an approximate solution to the problem. Fully polynomial randomized approximation schemes are efficient algorithms for obtaining such approximations.

Definition 2.4.2. ([Va] p.100) A *fully polynomial randomized approximation scheme* (fpras) is a probabilistic algorithm which given an error parameter ϵ and a confidence parameter δ outputs an estimate with relative error at most ϵ with confidence at least δ in time bounded by some polynomial in $\frac{1}{\epsilon}, \frac{1}{\delta}$ and the length of the input.

Now, suppose that we have a population of combinatorial objects and we wish to generate elements from it uniformly at random. Clearly, this would be a trivial problem if one could easily generate any item at will from an enumerated list. But as we have seen, it is not always feasible to get an exact count of the population.

Further, it might be difficult to generate elements from it. Here we would also be satisfied with an "almost random" member.

These two seemingly disparate problems have been shown to be equivalent for sets defined by self reducible relations [Si],[SiJe]. Thus, in such instances one can formulate an approximate counting problem in terms of an almost uniform generation problem.

A particularly elegant approach to almost uniform generation is the Markov chain technique. In the Markov chain technique, one constructs a Markov chain whose state space is the set of structures in question and whose stationary distribution is uniform on the state space. One then simulates the chain until it is sufficiently close to stationarity and accepts the terminal state as the desired "random" element.

The feasibility of the above technique relies heavily on two conditions. First, the transitions of the Markov chain should be easy to simulate. Secondly, the Markov chain should converge rapidly to stationarity. Chains which converge rapidly to stationarity are called rapidly mixing. This will be the subject of the next section.

5. Convergence to Stationarity

Analysis of the rate of convergence of the Markov chain implemented in a random generation scheme is crucial to determining its efficiency. Classical techniques have relied on the analysis of the second largest eigenvalue of the transition matrix, but such methods are impractical in most cases, especially when the chain has a large state space. However, recently powerful new tools have been developed to tackle the task of analyzing the mixing properties of Markov chains.

The first steps taken in this direction were made by Jerrum and Sinclair [SiJe]. They showed that the rate of convergence of a Markov chain could be analyzed by examining the underlying digraph of the chain. First they defined a quantity, conductance, and related it to the second largest eigenvalue of the chain. Then they obtained a lower bound for the conductance by a technique called canonical paths. This enabled them to get a bound on the mixing time of the chain. For a detailed history of these developments see Vazirani [Va].

We will now state basic definitions and theorems needed for the subsequent chapters. Our exposition will follow that of Vazirani [Va] which is based on the work of Mihail [Mi].

Before we make precise what we mean when we say that a Markov chain is rapidly mixing we need the following definition.

Definition 2.5.1. A Markov chain with transition matrix P and state space S is *strongly aperiodic* if $P_{ii} \geq \frac{1}{2}$ for all $i \in S$.

Let X be an irreducible, strongly aperiodic Markov chain with state space $V = \{1, 2, \cdots, N\}$, transition matrix P and stationary distribution π, and recall that if p_0 is any initial distribution, the the distribution of the chain after t steps is given by $p_t = p_0 P^t$.

Definition 2.5.2. ([Va] p.102) Let $d_1(t) = \sum_{i=1}^{N} |p_t(i) - \pi_i|$. Then we say a Markov chain is *rapidly mixing* if $d_1(t) \leq \epsilon$ for $t = \log(\frac{1}{\epsilon})\text{poly}(\log N)$, for some polynomial poly.

Definition 2.5.3. Let $S \subset V$. Then the *conductance*, $\Phi_P(S)$ of S, is defined to be

$$\Phi_P(S) = \frac{\sum_{i \in S} \sum_{j \in V \setminus S} w_{ij}}{\sum_{i \in S} \pi_i} = \frac{\sum_{i \in S} \sum_{j \in V \setminus S} w_{ij}}{\sum_{i \in S} \sum_{j \in V} w_{ij}},$$

and the conductance Φ_P of P is :

$$\Phi_P = \min_{S \subset V : \sum_{i \in S} \pi_i \leq \frac{1}{2}} \Phi_P(S).$$

We have the following proposition relating conductance to the L_2 distance, $d_2(t) = \sum_{i=1}^{N} (p_t(i) - \pi_i)^2$, between p_t and π.

Proposition 2.5.4. ([Va] p.103) *For any irreducible and strongly aperiodic stochastic matrix P, and any initial distribution p_0 we have:*

$$d_2(t+1) \leq (1 - \Phi_P^2) d_2(t)$$

Hence:

$$d_2(t) \leq (1 - \Phi_P^2)^t d_2(0).$$

The fact that $d_2(0) \leq 2$ and the Cauchy-Schwartz inequality gives

$$d_1(t) \leq \sqrt{N d_2(t)} \leq \sqrt{2N (1 - \Phi_P^2)^t}.$$

Now, if we can obtain a lower bound on the conductance, we can obtain an upper bound on $d_1(t)$ and hence a lower bound on the mixing time. We need the following definitions.

Definition 2.5.5. ([Va] p.112) The conductance of an unweighted, undirected, regular graph is given by

$$\Phi = \min_{|S| \leq \frac{|V|}{2}} \left\{ \frac{|E_{S,\bar{S}}|}{|E_S|} \right\}.$$

Note that this definition is a special case of Definition 2.5.3. Here, $|E_{S,\bar{S}}|$ denotes the number of edges between S and $\bar{S}$ and $|E_S| = \sum_{v \in S} \deg(v)$.

Definition 2.5.6. ([Va] p.112) The *edge magnification of a graph* is given by

$$\mu = \min_{|S| \leq \frac{|V|}{2}} \left\{ \frac{|E_{S,\bar{S}}|}{|S|} \right\}.$$

Another key concept in determining the mixing properties of a graph is congestion. Let G be a digraph. For every ordered pair, (u, v), of vertices of G, fix a path from u to v called the *canonical path* from u to v. The *congestion* of an edge e is defined to be the number of canonical paths that contain e.

The argument of Vazirani's that follows relating conductance and congestion assumes that the graph G is regular. Later we will generalize these results.

Proposition 2.5.7. ([Va] p.114) *Let $G(V, E)$ be a (regular) directed graph. Let*

$N = |V|$. If αN is the maximum congestion through an edge then

$$\mu \geq \frac{1}{2\alpha}.$$

Proof: Given a cut $(S, \bar{S})$, there are $|S||\bar{S}|$ paths that cross from S to $\bar{S}$, each of which must use at least one edge in $E_{S,\bar{S}}$. Since the number of edge crossings from S to $\bar{S}$ is $\left|E_{S,\bar{S}}\right|$ and αN is the maximum congestion for any edge, the number of edge traversals does not exceed $\left|E_{S,\bar{S}}\right| \alpha N$. Hence,

$$\left|E_{S,\bar{S}}\right| \alpha N \geq |S||\bar{S}| \geq |S| \frac{N}{2}.$$

Therefore

$$\frac{\left|E_{S,\bar{S}}\right|}{|S|} \geq \frac{1}{2\alpha},$$

and since this is true for all cuts $(S, \bar{S})$ we have

$$\mu \geq \frac{1}{2\alpha}. \qquad \square$$

We now examine the case where G is not regular. Utilizing bounds on the degrees of G we obtain the following bound on the conductance.

Proposition 2.5.8. *Let $G = (V, E)$ be a graph with $|V| = N$ such that*

$$\frac{N}{2}(1 - \varepsilon) \leq \deg(v) \leq \frac{N}{2}(1 + \varepsilon)$$

for all of its vertices v. If αN is the maximum congestion through an edge then

$$\Phi \geq \left(\frac{1-\varepsilon}{(1+\varepsilon)^2}\right)\frac{1}{N\alpha}.$$

Proof: Let $S \subset V$ with $\sum_{i\in S}\pi_i \leq \frac{1}{2}$ and for any $T \subset V$ let $D(T) = \sum_{i\in T}\deg(i)$. Then $D(S) \leq \frac{1}{2}D(G)$ and $D(\bar{S}) > \frac{1}{2}D(G)$. By assumption we have

$$|\bar{S}|\frac{N}{2}(1-\epsilon) \leq D(\bar{S}) \leq |\bar{S}|\frac{N}{2}(1+\epsilon).$$

Hence,

$$|\bar{S}|\frac{N}{2}(1+\epsilon) \geq D(\bar{S}) \geq \frac{1}{2}D(G) \geq \frac{1}{2}N\frac{N}{2}(1-\epsilon).$$

Thus

$$|\bar{S}| \geq \left(\frac{\frac{N}{2}(1-\varepsilon)}{\frac{N}{2}(1+\varepsilon)}\right)\frac{N}{2}$$

$$= \left(\frac{1-\varepsilon}{1+\varepsilon}\right)\frac{N}{2}.$$

Hence

$$\left|E_{S,\bar{S}}\right|\alpha N \geq |S||\bar{S}| \geq |S|\left(\frac{1-\varepsilon}{1+\varepsilon}\right)\frac{N}{2}.$$

Thus

$$\frac{\left|E_{S,\bar{S}}\right|}{|S|} \geq \left(\frac{1-\varepsilon}{1+\varepsilon}\right)\frac{1}{2\alpha}.$$

Since this is true for all $S \subset V$ with $\sum_{i\in S}\pi_i \leq \frac{1}{2}$, we have

$$\Phi = \min_{S\subset V:\sum_{i\in S}\pi_i\leq\frac{1}{2}}\left\{\frac{\left|E_{S,\bar{S}}\right|}{|E_S|}\right\}$$

$$\geq \min_{S\subset V:\sum_{i\in S}\pi_i\leq\frac{1}{2}}\left\{\frac{|E_{S,\bar{S}}|}{\frac{N}{2}(1+\varepsilon)|S|}\right\}$$

$$\geq\left(\frac{2}{N(1+\varepsilon)}\right)\min_{S\subset V:\sum_{i\in S}\pi_i\leq\frac{1}{2}}\left\{\frac{|E_{S,\bar{S}}|}{|S|}\right\}$$

$$\geq\left(\frac{2}{N(1+\varepsilon)}\right)\left(\frac{1-\varepsilon}{1+\varepsilon}\right)\frac{1}{2\alpha}$$

$$=\left(\frac{1-\varepsilon}{(1+\varepsilon)^2}\right)\frac{1}{N\alpha}. \qquad \square$$

We conclude by noting Definitions 2.5.5 and 2.5.6 in the case of a regular graph of degree $\frac{n}{2}$ is equivalent to Proposition 2.5.8 in the case $\varepsilon = 0$. In this case we have,

$$\Phi = \min_{|S|\leq\frac{|V|}{2}}\left\{\frac{|E_{S,\bar{S}}|}{|E_S|}\right\}$$

$$= \min_{|S|\leq\frac{|V|}{2}}\left\{\frac{|E_{S,\bar{S}}|}{\frac{N}{2}|S|}\right\}$$

$$= \frac{2}{N}\min_{|S|\leq\frac{|V|}{2}}\left\{\frac{|E_{S,\bar{S}}|}{|S|}\right\}$$

$$= \frac{2}{N}\mu$$

$$\geq \frac{2}{N}\frac{1}{2\alpha}$$

$$= \frac{1}{N\alpha}.$$

CHAPTER III

APPLICATIONS TO STEINHAUS GRAPHS

1. Introduction

In this chapter we investigate the mixing properties of random generalized Steinhaus graphs. A basic question in the theory of random graphs is: Given a graph property, what is the probability that a graph has this property? If this number is one we say almost all graphs have the property. In this chapter we show that almost all generalized Steinhaus graphs are rapidly mixing.

In Section 2 we state the two basic models of the theory of random graphs and state some well known results. In Section 3 we define Steinhaus graphs and generalized Steinhaus graphs and give some recent results of Brand and other authors. Finally, in Section 4 we employ the results of Chapter 2 to show that almost all generalized Steinhaus graphs are rapidly mixing.

2. Random graphs

The theory of the evolution of random graphs which grew from the two seminal papers of Erdős and Rényi, [ErRe1], [ErRe2] (see [Pa]), is a striking example of the use of the probabilistic method in mathematics. We will not be concerned with the history of the theory but will only state the two basic models and some well known results. For more background and results see [Bo2] and [Pa].

In the first model we will consider, the sample spaces Ω_n consisting of all labeled graphs G of order n. Specifically, for each positive integer n and number $p = p(n)$ with $0 < p < 1$, the probability of a graph $G \in \Omega_n$ with q edges is given by

$$P(G) = p^q(1-p)^{\binom{n}{2}-q}.$$

It is often convenient to view the set of pairs of vertices of G as a sequence of $\binom{n}{2}$ Bernoulli trials and consider p as the probability of an edge. This model of random graph theory is refer to as either *Model A*, [Pa] $\mathcal{G}\{n, P((\text{edge})) = p(n)\}$ or $\mathcal{G}_p(n)$ [Bo2].

In the second basic model, the sample spaces $\Omega_{n,q}$ consist of all labeled graphs G of order n and size $q = q(n)$, that is with $q(n)$ edges. In this model the probability of each graph G is given by

$$P(G) = \binom{\binom{n}{2}}{q}^{-1}.$$

This model is referred to as either *Model B*, $\mathcal{G}(n, M(n))$ or $\mathcal{G}_M(n)$ where $M(n) = q$.

In this chapter we will be using Model A. For more information on these models and others see [Bo2], [Lu].

Let Q be a property of graphs and consider the set A_n of graphs of order n that possess property Q. If $\lim_{n\to\infty} P(A_n) = 1$ then we say that *almost all graphs have property* Q. A very useful property of graphs from which many results easily follow is property P_k.

Definition 3.2.1. ([Bo2] p.40) A graph $G = (V, E)$ has *property* P_k if whenever W_1, W_2 are sets of at most k vertices each then there is a vertex $z \in V - W_1 \cup W_2$ joined to every vertex in W_1 and none in W_2.

In Model A, if p is fixed then almost every graph has P_k ([Pa] p.13). However, Bollobás [Bo2] proves a more general result.

Proposition 3.2.2. ([Bo2] p.40) *Suppose $M = M(n)$ and $p = p(n)$ are such that for every $\varepsilon > 0$ we have*

$$Mn^{-2+\varepsilon} \to \infty \qquad \text{and} \qquad (N - M)n^{-2+\varepsilon} \to \infty,$$

$$pn^{\varepsilon} \to \infty \qquad \text{and} \qquad (1 - p)n^{\varepsilon} \to \infty.$$

Then for every fixed $k \in \mathbb{N}$ almost every graph in Model B has P_k and almost every graph in Model A has P_k.

From this proposition it follows [Bo2] that if Q is any property of graphs given by a first order sentence, then either Q holds for almost every graph in Model A and Model B or Q fails for almost every graph in Model A and Model B.

In particular, in Model A with p and k fixed, we have [Pa]

- Almost all graphs have diameter 2.
- Almost all graphs are k-connected.
- Almost all graphs contain a subgraph of order k as an induced subgraph.
- Almost all graphs are nonplanar.
- Almost all graphs are locally connected.

An important property possessed by almost all graphs which can't be expressed by a first order sentence is given by the following proposition.

Proposition 3.2.3. ([Pa] p.66) *Let $G = (V, E)$ be a graph, $|V| = n, \varepsilon > 0$ and suppose $\omega_n \to \infty$ arbitrarily slowly. If the probability of an edge is*

$$p = \omega_n \frac{\log n}{n},$$

then almost every graph satisfies

$$(1-\varepsilon)pn < deg(v) < (1+\varepsilon)pn$$

for each of its vertices v.

Proof: For each $1 \le i \le n$ let

$$X_i(G) = \begin{cases} 0 & \text{if } (1-\varepsilon)pn < \deg(i) < (1+\varepsilon)pn \\ 1 & \text{otherwise.} \end{cases}$$

Then $X(G) = \sum_{i=1}^{n} X_i(G)$ is the number of vertices of G whose degrees lie outside the interval $((1-\varepsilon)pn, (1+\varepsilon)pn)$. The expected value of X is

$$E(X) = n \sum_{k:|k-pn|\ge p\varepsilon} \binom{n-1}{k} p^k (1-p)^{n-1-k}.$$

Then by using estimates on the tail of the binomial distribution one can easily see that $E(X) \to 0$. □

We close by mentioning a result of Chung, Graham and Wilson. In [CGW] the authors show the equivalence of a set of graph properties possessed by almost all graphs in $\mathcal{G}_{\frac{1}{2}}(n)$ in the sense that any graph possessing any one of them must necessarily possess all of the others. Such graphs are called *quasi-random*. Let us consider the the properties $P_2(t), P_3$.

$$P_2(t) : e(G) \geq (1 + o(1))\tfrac{n^2}{4}, \qquad N_G(C_t) \leq (1 + o(1))\left(\tfrac{n}{2}\right)^t$$

where $N_G(C_t)$ denotes the number of occurrences of the cycle of length t as a subgraph of G and $e(G)$ denotes the number of edges of G

$$P_3 : e(G) \geq (1 + o(1))\tfrac{n^2}{4}, \qquad \lambda_1 = (1 + o(1))\tfrac{n}{2}, \qquad \lambda_2 = o(n)$$

where λ_i are the eigenvalues of the adjacency matrix of G and $|\lambda_1| \geq \cdots \geq |\lambda_n|$.

Proposition 3.2.4. *For each n, let Q_n be a quasi-random graph with n vertices and let G_n be the graph obtained by adjoining a tail of length $\sqrt{n}$ to Q_n. Then G_n is quasi-random but not rapidly mixing.*

Proof: For each n, the number of edges in G_n is

$$\begin{aligned} e(G_n) &= e(Q_n) + \sqrt{n} \\ &\geq (1 + o(1))\frac{n^2}{4} + \sqrt{n} \\ &= (1 + o(1))\frac{(n + \sqrt{n})^2}{4} \end{aligned}$$

and the number of 4-cycles is

$$N_{G_n}(C_4) = N_{Q_n}(C_4)$$

$$\leq (1+o(1))\left(\frac{n}{2}\right)^4$$

$$= (1+o(1))\left(\frac{n+\sqrt{n}}{2}\right)^4 .$$

Hence G_n is quasi-random. But certainly G_n is not rapidly mixing as it takes at least $\sqrt{n}$ steps for a random walk commencing at the end vertex to reach a vertex in Q_n. □

3. Steinhaus graphs

Steinhaus graphs are a class of graphs whose adjacency matrices satisfy a simple recurrence relation. A defining property of Steinhaus graphs is that they are completely determined by adjacencies of a single vertex. In this section we will define Steinhaus graphs and generalized Steinhaus graphs and note some of the properties possessed by almost all of them. The results of this section are taken from [Br1], [BCDJ], [BrJa] and [BrMo] where generalized Steinhaus graphs are first defined.

Let $(a_{1,j})_{j=1}^n$ be a string of 0's and 1's. We define $a_{i,j}$ for $1 \leq i < j \leq n$ inductively by the relation $a_{i,j} \equiv a_{i-1,j-1} + a_{i-1j} \mod 2$. The numbers $a_{i,j}, 1 \leq i \leq n-1, 2 \leq j \leq n$ are referred to as a *Steinhaus triangle of order* n. We complete $a_{i,j}$ to an $n \times n$ matrix by setting $a_{i,i} = 0$ for $1 \leq i \leq n$ and setting $a_{i,j} = a_{j,i}$ for $i > j$. A graph whose adjacency matrix is so generated is referred to as a *Steinhaus graph* and the string of 0's and 1's, $(a_{1,j})_{j=1}^n$ is called the *generating string* of both the graph and the triangle.

Note that by specifying a generating string, we are specifying the adjacencies of the vertex with label one. It is easy to see that a Steinhaus graph is also determined by specifying the adjacencies of any other vertex.

Example 3.3.1. Consider the generating string $(a_{1,j})_{j=2}^{8} = \{1,0,1,0,1,1,0\}$. The Steinhaus triangle and adjacency matrix associated with this string are

$$\begin{array}{ccccccc}
1 & 0 & 1 & 0 & 1 & 1 & 0 \\
 & 1 & 1 & 1 & 1 & 0 & 1 \\
 & & 0 & 0 & 0 & 1 & 1 \\
 & & & 0 & 0 & 1 & 0 \\
 & & & & 0 & 1 & 1 \\
 & & & & & 1 & 0 \\
 & & & & & & 1
\end{array}
\qquad
\begin{pmatrix}
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 & 0
\end{pmatrix}.$$

In [BrMo], Brand and Morton develop the following generalization of Steinhaus graphs. Let $s : \mathrm{N} \to \mathrm{N} - \{1\}$ be a function. A *generalized Steinhaus triangle* of order n and type s is the upper triangular portion of an $n \times n$ array $A = (a_{i,j})$ whose entries satisfy

$$a_{i,j} = \sum_{r=0}^{s(i)-1} c_{r,i,j} a_{i-1,j-r} \pmod 2$$

where $2 \leq i \leq n-1, i + s(i) - 1 \leq j \leq n, c_{r,i,j} \in \{0,1\}$ and $c_{s(i)-1,i,j} = 1$. As in the case of Steinhaus graphs, we define $a_{i,i} = 0$ for $1 \leq i \leq n$ and set $a_{i,j} = a_{j,i}$ for $i > j$. A graph with such an adjacency matrix is referred to as a *generalized Steinhaus graph*.

Example 3.3.2. Let $n = 8, s(2) = 4, s(3) = 3, s(4) = 4, s(5) = 2, s(6) = 3, s(7) = 2$ and $c_{r,i,j} = 1$ if $r = 0$ or $s(i) - 1$. Otherwise $c_{r,i,j} = 0$. Then below is the generalized Steinhaus triangle of the generating string in boldface.

c	$s(i)$							
		1	**0**	**0**	**1**	**1**	**0**	**1**
$(1,0,0,1)$	4		**0**	**1**	0	1	0	0
$(1,0,1)$	3			**1**	0	0	0	1
$(1,0,0,1)$	4				**1**	**1**	1	1
$(1,1)$	2					0	0	0
$(1,0,1)$	3						**1**	0
$(1,1)$	2							1

As in [BrMo] we define a probability measure on the set of generalized Steinhaus graphs by requiring $\Pr[a_{i,j} = 1] = \frac{1}{2}$ for each $a_{i,j}$ in the generating string so that each graph occurs with the same probability. It then follows that $\Pr[a_{i,j} = 1] = \frac{1}{2}$ for all $1 \leq i < j \leq n$. We will also assume that $c_{0,i,j} = 1$ for $2 \leq i \leq n-1, i + s(i) - 1 \leq j \leq n$. Note that with this additional restriction, when $s \equiv 2$ we generate Steinhaus graphs.

The properties of random Steinhaus graphs and random generalized Steinhaus graphs have been investigated by Brand and other authors. The first paper to address a question of this nature was [Br1] in which Brand answered in the affirmative Brigham's and Dutton's [BrDu] conjecture that almost all Steinhaus graphs have diameter two where $\Pr[a_{1,j} = 1] = \frac{1}{2}$. In [BCDJ] Brand, Curran, Das and Jacob generalize this result to the case where $0 < \Pr[a_{1,j} = 1] < 1$. A much more general result is obtained in [BrJa] in which Brand and Jackson show that the theory of random Steinhaus graphs is first order complete and identical with the first order theory of random graphs. Thus a first order statement is true for almost all graphs if and only if it is true for almost all Steinhaus graphs. Finally in [BrMo], Brand and Morton extend these results to generalized Steinhaus graphs.

4. Almost all generalized Steinhaus graphs are rapidly mixing

Let us recall what it means to say a set of events is independent.

Definition 3.4.1. ([Bil] p.48) A finite collection of events $A_1, A_2, \cdots, A_n$ is *independent* if

$$\Pr\left[A_{k_1} \cap \cdots \cap A_{k_j}\right] = \Pr\left[A_{k_1}\right] \cdots \Pr\left[A_{k_j}\right]$$

for $2 \leq j \leq n$ and $1 \leq k_1 < \cdots < k_k \leq n$.

Let us fix i and consider the events

$$[a_{1,i} = 1], [a_{2,i} = 1], \cdots, [a_{i-1,i} = 1], [a_{i,i+1} = 1], [a_{i,i+2} = 1], \cdots, [a_{i,n} = 1].$$

That is we consider the events that vertex i is adjacent to another vertex. Our aim is to show that this is an independent collection of events. Now, since $\Pr\left[a_{i,j} = 1\right] = \frac{1}{2}$ for all $1 \leq i < j \leq n$ this is equivalent to showing that

$$\Pr([a_{1,i} = I_1] \cap \cdots \cap [a_{i-1,i} = I_{i-1}] \cap [a_{i,i+1} = I_i] \cap \cdots \cap [a_{i,n} = I_{n-1}]) = \frac{1}{2^{n-1}}$$

for any $I = \langle I_1, \cdots, I_{i-1}, I_i, \cdots, I_{n-1} \rangle \in \{0,1\}^{n-1}$.

In [BrMo], Brand and Morton developed a scheme for numbering the entries in the generalized Steinhaus triangle with the following properties.

- No two elements of the generating string have the same number.
- Each entry that is not in the generating string has the same number as some entry in the generating string.
- Changing an entry $a_{i,j}$ in the generating string will change all of the entries with the same number as $a_{i,j}$ and leave unchanged any entry with a number less than $a_{i,j}$.
- For each $2 \leq j \leq n, \phi_j(i)$ is an increasing function for $1 \leq i \leq j-1$ where $\phi_j(i)$ denotes the number of $a_{i,j}$.

Additionally, since $c_{0,i,j} = 1$ for $2 \leq i \leq n-1, i+s(i)-1 \leq j \leq n$, we have the following property.

- Changing an entry $a_{1,j}$ in the generating string will change the entries $a_{i,j}$ for $2 \leq i \leq j-1$.

Thus there are $n-1$ positions in the generating string that will determine the entries $a_{1,i}, \cdots, a_{i-1,i}, a_{i,i+1}, \cdots, a_{i,n}$. Hence for any assignment of values to the entries in the generating string outside these $n-1$ positions and any $I \in \{0,1\}^{n-1}$ there is only one choice for these $n-1$ positions which will give

$$a_{1,i} = I_1, \cdots, a_{i-1,i} = I_{i-1}, a_{i,i+1} = I_i, \cdots, a_{i,n} = I_{n-1}.$$

Hence the desired probability is clearly $\frac{1}{2^{n-1}}$. Thus we have the following proposition.

Proposition 3.4.2. *For each $i = 1, \cdots, n$ the events*

$$[a_{1,i} = 1], [a_{2,i} = 1], \cdots, [a_{i-1,i} = 1], [a_{i,i+1} = 1], [a_{i,i+2} = 1], \cdots, [a_{i,n} = 1]$$

are independent.

Thus as an analog to Palmer's proposition on the degrees of almost all graphs, we have the following proposition on the degrees of almost all generalized Steinhaus graphs.

Proposition 3.4.3. (See [Pa] p.66) *Let $\varepsilon > 0$. Then almost all generalized Steinhaus graphs satisfy*

$$\frac{n}{2}(1 - \epsilon) < degd(v) < \frac{n}{2}(1 + \epsilon)$$

for all of their vertices.

Finally, with the above proposition and the last result of Chapter 2, we have the following lower bound on the conductances of almost all generalized Steinhaus graphs.

Proposition 3.4.4. *For almost all generalized Steinhaus graphs, the conductance Φ satisfies*

$$\Phi \geq \left(\frac{1 - \varepsilon}{(1 + \varepsilon)^2} \right) \frac{1}{N\alpha}.$$

where $N\alpha$ is the maximum congestion of an edge.

We now estimate the mixing rate of almost all generalized Steinhaus graphs. We will use the method of canonical paths. To do so we need the following proposition.

Proposition 3.4.5. *For almost all generalized Steinhaus graphs G, given $x, y \in V$ there are at least $\frac{|V|}{64}$ vertices connected to both x and y.*

Proof: In [BrMo] it is shown that given $T_1, T_2 \subset V$, $|T_1| = |T_2| = k$ there is a "good set" S of size at least $\frac{n}{8k^2}$ such that the events $\{a(v_1, v_{t_1}), a(v_2, v_{t_2}) \mid v_1, v_2 \in S, v_{t_1} \in T_1, v_{t_2} \in T_2\}$ are independent. We will call such a set independent for T_1 and T_2

Let $x, y \in V, T_1 = \{x\}, T_2 = \{y\}$. Then there is a set S of size at least $\frac{n}{8}$ that is independent for $\{x\}$ and $\{y\}$. For each $s \in S$, let $X_s = 1$ if s is adjacent to both x and y; otherwise, let $X_s = 0$. Since S is independent for $\{x\}$ and $\{y\}, \{X_s \mid s \in S\}$ is a sequence of independent Bernoulli trials with $\Pr[X_s = 1] = \frac{1}{4}$ where we regard the event $X = 1$ as a success. Thus the number X of successes is a binomial random variable with parameters $\left(|S|, \frac{1}{4}\right)$ and expected value at least $\frac{n}{32}$.

We now obtain an upper bound for $\Pr\left[X \leq \frac{n}{64}\right]$.

$$\Pr\left[X \leq \frac{n}{64}\right] \leq \sum_{i=0}^{\lfloor n/64 \rfloor} \binom{n/8}{i} \left(\frac{1}{4}\right)^i \left(\frac{3}{4}\right)^{n/8-i}$$

$$\leq \frac{n}{64} \binom{n/8}{n/64} \left(\frac{1}{4}\right)^{n/64} \left(\frac{3}{4}\right)^{7n/64}$$

$$\sim \left(\frac{n}{64}\right) \frac{\left(\frac{n}{8}\right)^{n/8} \sqrt{\frac{n}{8}}}{\sqrt{2\pi} \left(\frac{n}{64}\right)^{n/64} \sqrt{\frac{n}{64}} \left(\frac{7n}{64}\right)^{7n/64} \sqrt{\frac{7n}{64}}} \left(\frac{1}{4}\right)^{n/64} \left(\frac{3}{4}\right)^{7n/64}$$

$$= \sqrt{\frac{n}{112\pi}} \left(\frac{\left(\frac{1}{8}\right)^{n/8}}{\left(\frac{1}{64}\right)^{n/64} \left(\frac{7}{64}\right)^{7n/64}} \right) \left(\frac{1}{4}\right)^{n/64} \left(\frac{3}{4}\right)^{7n/64}$$

$$= \sqrt{\frac{n}{112\pi}} \left(\frac{8^{n/8}}{7^{7n/64}}\right) \left(\frac{1}{4}\right)^{n/64} \left(\frac{3}{4}\right)^{7n/64}$$

$$= \sqrt{\frac{n}{112\pi}} \left(\frac{8^{n/8}}{4^{n/64}}\right) \left(\frac{3}{28}\right)^{7n/64}$$

$$= \sqrt{\frac{n}{112\pi}} \left(\frac{24 \cdot 2^{1/7}}{28}\right)^{7n/64}$$

$$< \sqrt{\frac{n}{112\pi}} \left(\frac{26.5}{28}\right)^{7n/64}$$

Thus the probability P that for some pair of vertices there are less than $\frac{n}{64}$ vertices adjacent to both satisfies

$$P \leq \binom{n}{2} \sqrt{\frac{n}{112\pi}} \left(\frac{26.5}{28}\right)^{7n/64}$$

$$\leq \left(\frac{n^{5/2}}{\sqrt{448\pi}}\right) \left(\frac{26.5}{28}\right)^{7n/64}$$

which clearly approaches 0 as $n \to \infty$.

Hence for almost all generalized Steinhaus graphs, for each pair of vertices there is set of vertices of size at least $\frac{n}{64}$ that are connected to both. □

To estimate the mixing rate of a generalized Steinhaus graph we will use the method of canonical paths. Let G be a generalized Steinhaus graph such that for every pair of vertices in G there is a set of vertices of size at least $\frac{n}{64}$ that are connected to both. For $1 \leq i < j \leq n$ choose a vertex $v_{i,j}$ that is adjacent to both i and j and different from $v_{i,l}$ for $j - \frac{n}{128} \leq l < j$ and $v_{k,j}$ for $i - \frac{n}{128} \leq k < i$. The canonical path from i to j will consist of the edges $(i, v_{k,l})$ and $(v_{k,l}, j)$. If $i > j$ we reverse the path from j to i.

Thus the maximum usage of an edge (i, x) is at most $2\frac{n}{n/128} = 256$. Hence for almost all generalized Steinhaus graphs,

$$\Phi \geq \left(\frac{1-\epsilon}{(1+\epsilon)^2}\right)\left(\frac{1}{256}\right).$$

For convenience, assume $\varepsilon < \sqrt{5} - 2$ so that

$$\Phi \geq \frac{1}{512}.$$

Thus for $0 < \varepsilon < 1$ we wish to find t such that

$$d_1(t) \leq \sqrt{2N\left(1 - \Phi_P^2\right)^t}$$

$$= \sqrt{2N\left(1 - 2^{-16}\right)^t}$$

$$\leq \varepsilon.$$

Taking logs of both sides we see we want

$$\frac{1}{2}\left[\log 2N + t\log\left(1 - 2^{-16}\right)\right] \leq \log\varepsilon$$

or

$$\log 2N + t\log\left(1 - 2^{-16}\right) \leq -2\log\left(\frac{1}{\varepsilon}\right).$$

Let $C = \left|\log\left(1 - 2^{-16}\right)\right|$. Thus

$$t \geq \frac{2\log(\frac{1}{\varepsilon}) + \log 2N}{C}$$

$$= \log\left(\frac{1}{\varepsilon}\right)\frac{\left[2+\frac{\log 2N}{\log\frac{1}{\varepsilon}}\right]}{C}.$$

It is sufficient that

$$t \geq \log\left(\frac{1}{\varepsilon}\right)\left(\frac{2}{C}+\frac{1}{C}\log 2N\right)$$

$$= \log\left(\frac{1}{\varepsilon}\right)\left(\frac{2+\log 2}{C}+\frac{\log N}{C}\right)$$

which is of the form

$$\log\left(\frac{1}{\varepsilon}\right)\operatorname{poly}(\log N).$$

Thus almost all generalized Steinhaus graphs are rapidly mixing.

CHAPTER IV

THE RANDOM GENERATION OF CYCLIC MENDELSOHN DESIGNS

1. Introduction

In this chapter we develop an algorithm to generate $2-(4l+1,4,1)$ cyclic Mendelsohn designs at random with a uniform distribution. The motivation for this algorithm is a conjecture of Brand and Huffman on the construction of cyclic Mendelsohn designs. In [BrHu], the authors construct $2-(13,4,1)$ and $2-(17,4,1)$ Mendelsohn designs from generic difference families by performing "switches" and ask whether all $2-(p^n,k,1)$ Mendelsohn design can be constructed in a similar manner. In this vein, we will construct $2-(4l+1,4,1)$ Mendelsohn designs at random by starting with a generic difference family and performing random switches.

The basis for this algorithm is the Markov chain technique. In Section 2, we introduce Mendelsohn designs, difference families and related facts. In Section 3, we construct the underlying graph of an irreducible, strongly aperiodic Markov chain. The vertices of this graph will be equivalence classes of difference families and the edges will correspond to switches. At each vertex we add enough loops so that after a sufficiently long random walk on the graph, it will occur with probability proportional to the number of difference families it represents. Thus, if one were to choose an arbitrary initial vertex, simulate the chain for an adequate number of steps, and choose a difference family at random from the class corresponding to the terminal vertex, the probability of this difference family would be nearly uniform. Finally, in Section 4 we outline our algorithm.

2. Mendelsohn Designs

Design theory is an intricate branch of combinatorics that has applications to statistics and computer science. We will not be concerned with the elementary theory of designs here, we will merely define the topics of interest.

Definition 4.2.1. ([BrHu]) A $2-(v,k,\lambda)$*Mendelsohn design* D is a multiset consisting of blocks $B=\{(v_1,v_2),(v_2,v_3),\cdots,(v_{k-1},v_k),(v_k,v_1)\}$ where $v_1,v_2,\cdots,v_k$ are distinct elements of a v-set $\mathcal{V}$ such that every ordered pair with distinct entries is in precisely λ blocks of D.

We have a concept of isomorphism for designs. Two designs are said to be *isomorphic* if there is a bijection on the v-sets which preserves block multiplicity and a design automorphism is an isomorphism of the design onto itself. We can now say what it means for a Mendelsohn design to be cyclic.

Definition 4.2.2. A Mendelsohn design is cyclic if it has v-set $\mathbb{Z}_v$ and translation by 1 is an automorphism.

In this chapter we will only consider Mendelsohn designs with $v=4l+1, k=4$

and $\lambda = 1$. In this case we have the obvious fact.

Proposition 4.2.3. *A cyclic* $2-(4l+1,4,1)$ *Mendelsohn design has* $(4l+1)l$ *blocks and* l *orbits.*

Proof: In a cyclic Mendelsohn design with $\lambda = 1$, every ordered pair of elements of $\mathbb{Z}_{4l+1}$ appears in exactly one block. Since there are $(4l+1)4l$ such pairs and the size of each block is four, there are $\frac{(4l+1)4l}{4} = (4l+1)l$ blocks; and since translation by one is an automorphism, there are $\frac{(4l+1)l}{4l+1} = l$ orbits. $\square$

For the sake of simplicity, we will henceforth abuse notation by writing the block $\{(v_1,v_2),(v_2,v_3),(v_3,v_4),(v_4,v_1)\}$ as $\{v_1,v_2,v_3,v_4\}$. Let us now consider the following example with $v = 13$.

Example 4.2.4.

$\{0,1,3,6\}$	$\{0,4,9,2\}$	$\{0,8,4,1\}$
$\{1,2,4,7\}$	$\{1,5,10,3\}$	$\{1,9,5,2\}$
$\{2,3,5,8\}$	$\{2,6,11,4\}$	$\{2,10,6,3\}$
$\{3,4,6,9\}$	$\{3,7,12,5\}$	$\{3,11,7,4\}$
$\{4,5,7,10\}$	$\{4,8,0,6\}$	$\{4,12,8,5\}$
$\{5,6,8,11\}$	$\{5,9,1,7\}$	$\{5,0,9,6\}$
$\{6,7,9,12\}$	$\{6,10,2,8\}$	$\{6,1,10,7\}$

$\{7,8,10,0\}$	$\{7,11,3,9\}$	$\{7,2,11,8\}$
$\{8,9,11,1\}$	$\{8,12,4,10\}$	$\{8,3,12,9\}$
$\{9,10,12,2\}$	$\{9,0,5,11\}$	$\{9,4,0,10\}$
$\{10,11,0,3\}$	$\{10,1,6,12\}$	$\{10,5,1,11\}$
$\{11,12,1,4\}$	$\{11,2,7,0\}$	$\{11,6,2,12\}$
$\{12,0,2,5\}$	$\{12,3,8,1\}$	$\{12,7,3,0\}$

Note that the blocks in each column are a translation by one of the block just above. Hence, we can consider this design as being generated by the starter blocks

$$\{\{0,1,3,6\},\{0,4,9,2\},\{0,8,4,1\}\}.$$

Now for each block in the above design, we form the quadruple consisting of the differences of consecutive elements. That is, if $B=\{a,b,c,d\}$ then we get the quadruple $(b-a,c-b,d-c,a-d)$. Doing this and taking the equivalence modulo 13 wherever we get a negative difference, we obtain

$$\mathcal{F}=\{(1,2,3,7),(4,5,6,11),(8,9,10,12)\}.$$

We call $\mathcal{F}$ a difference family for the design. Notice that the sum of the entries in each quadruple is equivalent to 0 modulo 13 and that each element of $\mathbb{Z}_{13}$ appears as an entry in a quadruple. This is not an accident. We will now formally define difference family and show that there is a one to one correspondence between difference families and Mendelsohn designs.

Definition 4.2.5. A $(4l+1,4)$-*difference family* $\mathcal{F}$, is a partition of $\mathbb{Z}_{4l+1}-\{0\}$ into cyclically ordered quadruples such that the sum of the entries in each quadruple is zero, and such that no element appears next to its inverse. Two difference families are considered equivalent if, neglecting order, they have the same quadruples.

Proposition 4.2.6. *There is a one to one correspondence between* $(4l+1,4)$-*difference families and* $2-(4l+1,4,1)$ *cyclic Mendelsohn designs.*

3. Development of algorithm

Recall that the Markov chain technique for almost uniform generation proceeds as follows. First one constructs an irreducible, strongly aperiodic Markov chain whose states are the structures of interest and where the transitions between states can be efficiently simulated. Then one chooses an arbitrary initial state, simulates the chain for an appropriate number of steps, then outputs the final state.

In this section, we develop an algorithm for the uniform generation of cyclic Mendelsohn designs employing the Markov chain technique. The majority of our work will lie in the construction of the underlying digraph of our Markov chain. To demonstrate that this is an efficient algorithm we would, of course, have to prove that convergence to stationarity is rapid. We cannot do this, although we feel that this is the case.

We first note that since we have a natural bijection between $2-(4l+1,4,1)$ cyclic Mendelsohn designs and $(4l+1,4)$ difference families, we could equivalently generate $(4l + 1, 4)$ difference families. We choose to generate difference families because, as we will soon see, the transitions between states are efficiently simulated.

Hence, the states of our chain will be labels for equivalence classes of difference families. Our algorithm will first generate a label for an equivalence class and then choose an element at random from the equivalence class. Recall that two difference families are considered to be equivalent if, neglecting order, they have the same quadruples. We will represent an equivalence class of difference families by first listing the elements of each quadruple in order then listing the quadruples in lexicographic order. We will call such a construct a *label*.

Example 4.3.1. The equivalence class containing

$$\{(3,1,4,5),(2,6,11,7),(9,10,12,8)\}$$

$$\{(4,1,5,3),(2,7,11,6),(9,10,8,12)\}$$

$$\{(1,3,5,4),(2,7,11,6),(10,8,9,12)\}$$

has label

$$\{(1,3,4,5),(2,6,7,11),(8,9,10,12)\}.$$

Note that in general a label is not a difference family.

Let L be a label and let $(a,b,c,d),(e,f,g,h)$ be two quadruples in L such that, without loss of generality, $a+b = e+f$. Then if we interchange a, b with e, f (and if necessary reorder the quadruples) we obtain another label, L'. Such an interchange we call a *switch*.

Example 4.3.2. We can obtain

$$\{(1,2,3,7),(4,5,6,11),(8,9,10,12)\}$$

from

$$\{(1,2,4,6),(3,5,7,11),(8,9,10,12)\}$$

by interchanging $4,6$ in the first quadruple with $3,7$ in the second.

Hence, the underlying graph $G = (V, E)$ of our Markov chain has vertex set $V = \{L \mid L \text{ is a label}\}$ and edge set $E \supseteq \{(L, L') \mid \exists \text{ a switch from } L \text{ to } L'\}$.

Now our Markov chain must be irreducible or equivalently our graph must be connected.

Conjecture 4.3.3. *$G = (V, E)$ is connected.*

We do not have a proof of this conjecture. However, since V has a natural lexicographic order we add edges to the lexicographically previous and lexicographically next vertices so that G is connected. Thus G will have edge set $E = \{(L, L') \mid \exists \text{ a switch from } L \text{ to } L' \text{ or } L \text{ and } L' \text{ are consecutive }\}$.

Our Markov chain must also be strongly aperiodic. We first show that it is aperiodic. Since the underlying graph of our chain is now connected, it is sufficient to show that it is not bipartite.

Proposition 4.3.4. *$G = (V, E)$ is not bipartite.*

Proof: Let k denote the number of quadruples. Consider the vertex:

$$\{(2n-1, 2n, -2n, -(2n-1)) : 1 \leq n \leq k\}.$$

We perform the following switches among the first two quadruples:

$$(1, 2, -2, -1), (3, 4, -4, -3) \longrightarrow (1, 3, -3, -1), (2, 4, -4, -2) \longrightarrow$$

$$(1, 4, -4, -1), (2, 3, -3, -2) \longrightarrow (1, 2, -2, -1), (3, 4, -4, -3).$$

Then this is a cycle of length three, so the graph can not be bipartite. □

However, it is not enough that our graph be aperiodic. We must ensure that it is strongly aperiodic, that is, $P_{ii} \geq \frac{1}{2}$ for all i. This will prevent the occurrence of oscillatory or "near-periodic" behavior [SiJe], [Mi]. As noted by Sinclair and Jerrum, including a large self-loop (or in our case multiple loops) to each vertex yields a graph with the same stationary distribution without slowing down convergence too much.

Thus we turn to the task of adding the proper number of loops to each vertex. Our purpose here is twofold. First, we add loops so that the probability of a vertex is proportional to the number of difference families that it represents. Secondly, we add loops for strong aperiodicity.

Definition 4.3.5. A quadruple q that contains both an element of $\mathbb{Z}_{4l+1} - \{0\}$ and its inverse will be referred to as a *zero quadruple.*

Proposition 4.3.6. *Let L be a label, $S(L)$ be the number of switches for L and p be the number of non-zero quadruples of L. Then the number of loops to add to L so that the probability of L is proportional to the number of difference families that L represents, and so that G is strongly aperiodic is $2 \cdot 3^p \left[3\binom{l}{2} + 2\right] - (S(L) + 2)$.*

Proof: We will first add enough loops so that each vertex occurs with the proper probability. Recall that the (stationary) probability of a vertex v in the case that the underlying graph is undirected is $\frac{d(v)}{TD}$ where $d(v)$ is the degree of vertex v and $TD = \sum_{v \in V} d(v)$ is the "total degree". Let v_p be a label which has exactly p non-zero quadruples. Then v_p represents $6^p 2^{l-p} = 3^p 2^l$ difference families. Thus the probability of choosing a difference family represented by this vertex is $\frac{d(v_p)}{TD}\frac{1}{3^p 2^l}$. Since we want difference families to be equiprobable, we must have

$$\frac{d(v_0)}{TD}\frac{1}{3^0 2^l} = \frac{d(v_1)}{TD}\frac{1}{3^1 2^l} = \frac{d(v_2)}{TD}\frac{1}{3^2 2^l} = \cdots = \frac{d(v_l)}{TD}\frac{1}{3^l 2^l}$$

or

$$3^l d(v_0) = 3^{l-1} d(v_1) = 3^{l-2} d(v_2) = \cdots = d(v_l).$$

Hence, $3^{l-p} d(v_p) = 3^l d(v_0)$ or $d(v_p) = \frac{3^l}{3^{l-p}} d(v_0) = 3^p d(v_0)$ for $0 \le p \le l$. Thus the degree of any vertex should be a multiple of $d(v_0)$. We will prove later that the maximum number of switches possible for a label is $3\binom{l}{2}$ and this maximum occurs when $p = 0$. Thus taking into account the edges to the previous and next labels we see that the maximum degree, $\Delta = 3\binom{l}{2} + 2$. Thus, we first add enough loops to each vertex to raise its degree to the maximum degree Δ, and then enough so that its degree is the appropriate multiple of Δ. Hence, to a label L with p non-zero quadruples, we add $3\binom{l}{2} + 2 - (S(L) + 2) = 3\binom{l}{2} - S(L)$ loops to raise the degree to Δ. We then add $3^{p-1}\left[3\binom{l}{2} + 2\right]$ loops for a total of $3^p\left[3\binom{l}{2} + 2\right] - (S(L) + 2)$ so that this label occurs with the proper probability. We then add enough loops to double the degree so that our graph is strongly aperiodic. Hence, we add a total of $2 \cdot 3^p\left[3\binom{l}{2} + 2\right] - (S(L) + 2)$ loops. □

Now, it might seem that adding such a large number of loops will slow down the rate of convergence of our algorithm, as it is likely that many loops would be chosen before an edge is encountered. We can overcome this difficulty by simulating the number of loops encountered until an edge is chosen. That is, we simulate a geometric random variable, where we interpret a success as choosing an edge.

The procedure for simulating a geometric random variable is an elementary exercise in probability, hence we include it here without proof.

Proposition 4.3.7. *Let X be a geometric random variable with probability of success p. Then we may simulate X with $\left\lfloor \frac{\log r}{\log 1-p} \right\rfloor + 1$ where r is chosen uniformly from $[0,1]$.*

Corollary 4.3.8. *We may simulate the number of steps to exit a vertex L with p non-zero quadruples by incrementing the iteration counter by*

$$\left\lfloor \log r \Big/ \log\left(1 - \frac{S(v) + 2}{2 \cdot 3^p\left[3\binom{k}{2} + 2\right]}\right) \right\rfloor + 1.$$

where r is chosen uniformly from $[0,1]$.

We now determine the maximum degree of G.

Proposition 4.3.9. *Fix a vertex v in the label graph with parameter k. Let n_j denote the number of quadruples having a pair of entries whose sum is j and let S denote the number of switches possible. Then,*

$$S = 2\binom{n_0}{2} + \frac{1}{2}\left[\binom{n_1}{2} + \cdots + \binom{n_{4k}}{2}\right].$$

Proof: Let us first count the number of switches between quadruples with a sum of zero. Certainly if $n_0 \leq 1$ there are no such switches. Suppose that v has two quadruples with a sum of zero: $(a, b, -b, -a), (c, d, -d, -c)$. There are two switches for this pair. Namely, interchange $b, -b$ with $c, -c$ to obtain $(a, c, -c, -a), (b, d, -d, -b)$; or interchange $b, -b$ with $d, -d$ to obtain $(a, d, -d, -a), (b, c, -c, -b)$. Thus, there are $2\binom{n_0}{2}$ switches involving quadruples with a sum of zero.

Suppose that both of (a, b, c, d) and (e, f, g, h) have a sum of j, say $c + d = g + h = j$ where $1 \leq j \leq 2k$. Then $a + b = e + f = 4k + 1 - j$. So, we can either switch c, d with g, h or switch a, b with e, f. In either case, we obtain the quadruples $(a, b, g, h), (e, f, c, d)$ after switching. Thus $n_j = n_{4k+1-j}$ and we need only count the switches involving pairs that have a sum between 1 and $2k$. Thus there are

$$\frac{1}{2}\left[\binom{n_1}{2} + \cdots + \binom{n_{4k}}{2}\right]$$

switches between pairs whose sum is nonzero. Hence, the total number is as claimed in the statement of the proposition. □

We now associate with each label v, a $4k+1$-tuple, $N = \langle n_0, n_1, \cdots, n_{4k} \rangle$ representing the distribution of sums. We would like to find the maximum value of S over all such N, but such a maximum is difficult to obtain. Instead, we find the maximum value of an equivalent function over a larger set of $4k+1$-tuples which contains those corresponding to the distribution of sums in labels. We then show that one N achieving this maximum comes from a label.

Lemma 4.3.10. *If v is a difference family then the distribution N satisfies:*

1) $0 \leq n_p \leq k$ for $0 \leq p \leq 4k$,

2) $2n_0 + n_1 + \cdots + n_{4k} = 6k$,

3) $n_j = n_{4k+1-j}$ for $j \neq 0$.

Proof: Since n_p is the the number of quadruples having a sum of p, it is clear that $0 \leq n_p \leq k$. Also as noted before, if a quadruple has a sum of $j, j \neq 0$, then it also has a sum of $4k+1-j$; hence, $n_j = n_{4k+1-j}$. Finally, if a quadruple has a pair of entries whose sum is zero, then the complementary pair also sums to zero. Since there are six pairs of elements for each quadruple, we have $2n_0 + n_1 + \cdots + n_{4k} = 6k$.

□

Our goal is to maximize S' subject to the conditions in lemma 4.3.10. We have

$$S = n_0(n_0 - 1) + \frac{1}{4}({n_1}^2 + {n_2}^2 + \cdots + {n_{4k}}^2 - n_1 - n_2 - \cdots - n_{4k})$$

$$= ({n_0}^2 - \frac{1}{2}n_0) + \frac{1}{4}(n_1^2 + n_2^2 + \cdots + {n_{4k}}^2 - (2n_0 + n_1 + n_2 + \cdots + n_{4k}))$$

$$= ({n_0}^2 - \frac{1}{2}n_0) + \frac{1}{4}(n_1^2 + n_2^2 + \cdots + {n_{4k}}^2) - \frac{3}{2}k$$

$$= ({n_0}^2 - \frac{1}{2}n_0) + \frac{1}{2}(n_1^2 + n_2^2 + \cdots + {n_{2k}}^2) - \frac{3}{2}k.$$

The last step follows from condition (3). We now rewrite condition (2) as

2) $n_0 + n_1 + \cdots + n_{2k} = 3k$,

and S as

$$S = \frac{1}{2}((2{n_0}^2 - n_0) + ({n_1}^2 + {n_2}^2 + \cdots + {n_{2k}}^2) - 3k)$$

$$= \frac{1}{2}((n_0 - 1)n_0 + ({n_0}^2 + {n_1}^2 + {n_2}^2 + \cdots + {n_{2k}}^2) - 3k).$$

Now note that $\langle n_0, n_1, \cdots, n_{2k}\rangle$ maximizes S if and only if it maximizes

$$S' = (n_0 - 1)n_0 + ({n_0}^2 + {n_1}^2 + \cdots + {n_{2k}}^2)$$

and that S' is invariant under permutations of $n_1, \cdots, n_{2k}$. Hence for convenience, we will assume $n_1 \geq n_2 \geq \cdots \geq n_{2k}$. That is, we reindex N so that the distribution of sums is decreasing. We now impose a fourth condition

4) if $n_0 + n_1 - k > 0$ then $n_{1+n_0+n_1-k} > 0$.

Proposition 4.3.11. *If v is a difference family and $n_0 + n_1 - k > 0$ then $n_{1+n_0+n_1-k} > 0$.*

Before we prove this proposition, we will prove the following lemma.

Lemma 4.3.12. *Let v be a difference family and q_1, q_2 be quadruples in v. Then q_1 and q_2 generate the same sums if and only if $q_2 = -q_1$.*

Proof of Lemma: Let $q_1 = (a, b, c, d), q_2 = (e, f, g, h)$. Clearly, if $q_2 = -q_1$ then they generate the same six sums. Now let us suppose that q_1 and q_2 generate the same six sums. Without loss of generality, we can assume that $a + b = e + f$. We now consider the possibilities for $a + c$. Certainly, $a + c \neq g + h$. Thus $a + c$ equals $e + g$,$e + h$,$f + h$ or $f + g$. Assume without loss of generality, that $a + c = e + g$. Thus, the only choices left for $a + d$ are $e + h$ and $f + g$. But if $a + d = e + h$ then

$$\left.\begin{array}{l} a+b=e+f \\ \\ a+c=e+g \\ \\ a+d=e+h \end{array}\right\} \Longrightarrow 3a+b+c+d = 3e+f+g+h \Longrightarrow a = e.$$

A contradiction. Thus $a + d = f + g$ and we can see

$$\left.\begin{array}{l} a+b=e+f \\ \\ a+c=e+g \\ \\ a+d=f+g \end{array}\right\} \Longrightarrow 3a+b+c+d = 2e+2f+2g \Longrightarrow 2a = 2(e+f+g) \Longrightarrow a = -h.$$

Then substituting $-h$ for a into the three equations above, we see that $b = -g, c = -f$ and $d = -e$. Hence, $q_1 = -q_2$. □

Proof of Proposition: If v has n_0 quadruples with a sum of 0 and n_1 quadruples with a sum of s_1 then there are at least $n_0 + n_1 - k$ quadruples with a sum of both 0 and s_1. Note that no pair of these quadruples can have another (nonzero) sum in common. For if they did, they would agree in all six sums and would be negatives of each other. But this is impossible as a quadruple with a sum of zero is of the form $(a, b, -b, -a)$, and the negative of a quadruple of this form is itself. □

In summary, we seek $N \in \mathcal{N}$ maximizing S' where $\mathcal{N}$ is the set of all $2k+1$-tuples satisfying

1) $0 \leq n_p \leq k, \quad 0 \leq p \leq 2k$,

2) $n_0 + n_1 + \cdots + n_{2k} = 3k$,

3) $n_1 \geq n_2 \geq \cdots \geq n_{2k}$,

4) if $n_0 + n_1 - k > 0$ then $n_{1+n_0+n_1-k} > 0$.

Proposition 4.3.13. *If $(n_0, n_1, \cdots, n_{2k})$ maximizes S' and $n_0 \neq k, n_1 \neq k$ then $S' \leq 3k^2$.*

The proof of this proposition requires the following lemma.

Lemma 4.3.14. *If N maximizes S', $n_0 \neq k, n_1 \neq k$ then N has the following form.*

(i) $n_0 + n_1 - k > 0$.

(ii) *$\exists p$ such that:*

a. $n_1 = \cdots = n_p$,

b. if $p \neq 1 + n_0 + n_1 - k$ *then* $n_1 > n_{p+1} > 0$,

c. if $p + 1 \neq 1 + n_0 + n_1 - k$ *then* $n_{p+2} = \cdots = n_{1+n_0+n_1-k} = 1$,

(iii) $n_l = 0$ for $l > 1 + n_0 + n_1 - k$;

(iv) $n_0 \leq \dfrac{n_1 - 1}{2}$.

Proof of lemma: Let $N = \langle n_0, n_1, \cdots, n_{2k} \rangle$ be a $2k+1$-tuple satisfying properties $(1) - (4)$ which maximizes S'. Suppose that $n_0 + n_1 - k \leq 0$ and l is the largest subscript such that $n_l > 0$. Consider

$$N' = \langle n_0, n_1 + 1, n_2, n_3, \cdots, n_{l-1}, n_l - 1, 0, 0, \cdots, 0 \rangle.$$

Then, clearly N' satisfies properties (1),(2) and (3). Now, ${n_0}' + {n_1}' - k \leq 1$. If ${n_0}' + {n_1}' - k \leq 0$, property (4) is satisfied vacuously. If ${n_0}' + {n_1}' - k = 1$, we need only to check that $n_2 > 0$. This follows clearly from property (2). An easy calculation shows $S'(N') > S'(N)$.

Now suppose that there are $1 < q < r \leq 2k$ such that $n_1 > n_q > n_r > 1$. Consider $N' = \langle n_0, n_1, \cdots, n_q + 1, \cdots, n_r - 1, \cdots \rangle$. Then N' satisfies properties (1)–(4) and an easy calculation shows that $S'(N') > S'(N)$.

Thus, for at most one subscript l can we have $n_1 > n_l > 1$. Let p be the largest subscript such that $n_p = n_1$. Then from property (4) it follows that if $p \neq 1 + n_0 + n_1 - k$ then $n_{p+1} > 0$. Similarly, if $p + 1 \neq 1 + n_0 + n_1 - k$ then $n_{p+1} = \cdots = n_{1+n_0+n+1-k} = 1$ follows from property (4).

Suppose $n_l > 0$ for $l > 1 + n_0 + n_1 - k$. Then $N' = \langle n_0, n_1 + 1, \cdots, n_p - 1, \cdots \rangle$ satisfies properties (1)–(4) and an easy calculation shows $S'(N') > S'(N)$.

Finally, consider $N' = \langle n_0 + 1, n_1 - 1, \cdots \rangle$. Then clearly N' satisfies properties (1)–(4). Evaluating, we find $S'(N') > S'(N)$ if and only if $4n_0 - 2n_1 + 2 > 0$ or $n_0 > \frac{n_1 - 1}{2}$. Thus, we must have $n_0 \leq \frac{n_1 - 1}{2}$. □

Proof of Proposition: We now calculate S' using Lemma 4.3.14.

$$S' = \begin{cases} n_0(n_0-1) + {n_0}^2 + p{n_1}^2 + {n_{p+1}}^2 + (n_0 + n_1 - k - p) & \text{if } n_{p+1} \neq 0; \\ \\ n_0(n_0-1) + {n_0}^2 + p{n_1}^2 & \text{if } n_{p+1} = 0. \end{cases}$$

Case 1. $n_{p+1} \neq 0$.

$$S' = n_0(n_0-1) + {n_0}^2 + p{n_1}^2 + {n_{p+1}}^2 + (n_0 + n_1 - k - p)$$

$$= 2{n_0}^2 + p{n_1}^2 + n_1 + {n_{p+1}}^2 - k - p$$

$$= p({n_1}^2 - 1) + 2{n_0}^2 + n_1 + {n_{p+1}}^2 - k.$$

We want $S' \leq 3k^2$ or

$$\text{(I)} \qquad p(n_1-1)(n_1+1) \leq 3k^2 - 2{n_0}^2 - n_1 - {n_{p+1}}^2 + k.$$

We wish to eliminate p from the above expression. From condition (2) we get

$$n_0 + pn_1 + n_{p+1} + (1 + n_0 + n_1 - k - (p+1)) = 3k$$

$$2n_0 + p(n_1-1) + n_1 + n_{p+1} - k = 3k$$

or

$$p(n_1 - 1) = 4k - 2n_0 - n_1 - n_{p+1}.$$

Hence,

$$\text{(II)} \quad p(n_1-1)(n_1+1) = 4kn_1 - 2n_0n_1 - {n_1}^2 - n_1n_{p+1} + 4k - 2n_0 - n_1 - n_{p+1}.$$

Substituting the expression obtained in equation II for $p(n_1-1)(n_1+1)$ into equation I and simplifying, we see that we need to show

$$3k^2 - 3k - 4kn_1 + 2n_0n_1 + n_1{}^2 + n_1n_{p+1} + 2n_0 + n_{p+1} - 2n_0{}^2 - n_{p+1}{}^2 \geq 0.$$

We factor the above and obtain

$$(3k - n_1)(k - n_1 - 1) + 2n_0(n_1 - n_0 + 1) + (n_{p+1} - 1)(n_1 - n_{p+1}) \geq 0.$$

It is clear that all of the terms in the above are nonnegative.

Case 2. $n_{p+1} = 0$.

Note that if $n_{p+1} = 0$ then $p = \dfrac{3k - n_0}{n_1}$. Substituting this value of p into S' and setting $S' \leq 3k^2$, we see upon factoring that we need to verify

$$3k(k - n_1) + n_0(n_1 + 1 - 2n_0) \geq 0.$$

Clearly, all of the terms in this expression are nonnegative. □

Proposition 4.3.15. *If $n_1 = k$ and $k \geq 3$ then the maximum value of S' occurs if $n_0 = 0$ or $n_0 = k$.*

Let $\mathcal{N}(i, j) = \{N \in \mathcal{N} : n_0 = i, n_1 = j\}$. We need the following two lemmas.

Lemma 4.3.16. *If k is odd and $N \in \mathcal{N}(l, k)$ maximizes S', then N is of one of the following forms.*

I. *If $0 \leq l \leq 2$ then*

(i) $n_1 = n_2 = k$,

(ii) $n_3 = k - l$,

(iii) $n_j = 0$ *for* $j > 3$.

II. *If* $2 < l \leq \frac{k+1}{2}$ *then*

(i) $n_1 = n_2 = k$,

(ii) $n_3 = k - 2(l-1)$,

(iii) $n_4 = \cdots = n_{l+1} = 1$,

(iv) $n_j = 0$ *for* $j > l+1$.

III. *If* $\frac{k+1}{2} < l \leq k$ *then*

(i) $n_1 = k$,

(ii) $n_2 = 2(k-l) + 1$,

(iii) $n_3 = \cdots = n_{l+1} = 1$,

(iv) $n_j = 0$ *for* $j > l+1$.

Lemma 4.3.17. *If k is even and $N \in \mathcal{N}(l,k)$ maximizes S', then N is of one of the following forms.*

I. *If* $0 \leq l \leq 2$ *then*

(i) $n_1 = n_2 = k$,

(ii) $n_3 = k - l$,

(iii) $n_j = 0$ *for* $j > 3$.

II. *If* $2 < l < \frac{k+2}{2}$ *then*

(i) $n_1 = n_2 = k$,

(ii) $n_3 = k - 2(l-1)$,

(iii) $n_4 = \cdots = n_{l+1} = 1$,

(iv) $n_j = 0$ *for* $j > l+1$.

III. *If* $l = \frac{k+2}{2}$ *then*

(i) $n_1 = k$,

(ii) $n_2 = k - 1$,

(iii) $n_3 = \cdots = n_{l+1} = 1$,

(iv) $n_j = 0$ *for* $j > l+1$.

IV. *If* $\frac{k+2}{2} < l \leq k$ *then*

(i) $n_1 = k$,

(ii) $n_2 = 2(k-l)+1$,

(iii) $n_3 = \cdots = n_{l+1} = 1$,

(iv) $n_j = 0$ *for* $j > l+1$.

The proofs of these lemmas are similar to the proof of Lemma 4.3.14. Thus for the sake of brevity, we will only prove part **I** of Lemma 4.3.16.

Proof of Lemma 4.3.13, part I: Suppose $0 \leq l \leq 2$ and $N \in \mathcal{N}(l,k)$ maximizes S'. Then from property (4), we have $n_{1+n_0} > 0$. Let s be the largest subscript such that $n_s > 0$. If $s > 3$ then $N' = \langle n_0+1, n_1, \cdots, n_{s-1}, n_s - 1, 0, \cdots, 0\rangle \in \mathcal{N}$ and an easy calculation shows $S'(N') > S'(N)$. Hence, $n_j = 0$ for $j > 3$. Similarly, if

$n_2 \neq k$, let $N' = (n_0, n_1, n_2 + 1, n_3 - 1, 0, \cdots, 0)$. Then, another easy calculation will show that $S'(N') > S'(N)$. Thus from property (2) we have $n_0 + n_1 + n_2 + n_3 = l + k + k + n_3 = 3k$ or $n_3 = k - l$. □

Proof of Proposition:

Let $f(l)$ denote the maximum value of S' over $\mathcal{N}(l,k)$. Using the above lemmas we calculate f and see that if k, is odd then

$$f(l) = \begin{cases} 3k^2 & \text{if } l = 0; \\ 3k^2 - 2k + 1 & \text{if } l = 1; \\ 3k^2 - 4k + 10 & \text{if } l = 2; \\ 3k^2 + 2(l-1)(3l - (2k+1)) & \text{if } 2 < l \leq \frac{k+1}{2}; \\ 3k^2 + 2(l-k)(3l - (k+2)) & \text{if } \frac{k+1}{2} < l \leq k \end{cases}$$

and if k is even,

$$f(l) = \begin{cases} 3k^2 & \text{if } l = 0; \\ 3k^2 - 2k + 1 & \text{if } l = 1; \\ 3k^2 - 4k + 10 & \text{if } l = 2; \\ 3k^2 + 2(l-1)(3l - (2k+1)) & \text{if } 2 < l < \frac{k+2}{2}; \\ \frac{1}{2}(5k^2 + 4) & \text{if } l = \frac{k+2}{2}; \\ 3k^2 + 2(l-k)(3l - (k+2)) & \text{if } \frac{k+2}{2} < l \leq k. \end{cases}$$

From the above it is clear that if $k \geq 3, S'$ has a maximum value of $3k^2$ and that this maximum is achieved if and only if $l = 0$ or $l = k$. □

Proposition 4.3.18. *If $n_0 = k$ then the maximum value of S' occurs for $n_1 = k$.*

Let $\mathcal{N}_0(k) = \bigcup_{j=0}^{k} \mathcal{N}(k,j)$. Again the proof of the following lemma is nearly idntical to the proof of lemma 4.3.14. Hence, we omit a proof.

Lemma 4.3.19. *If $N \in \mathcal{N}_0(k)$ achieves $\max\limits_{N \in \mathcal{N}_0(k)} S'(N)$, then N has the following form.*

(i) $n_0 = k$,

(ii) $\exists p$ *such that:*

a. $n_1 = n_2 = \cdots = n_p$,

b. *if* $p \neq 1 + n_1$ *then* $n_1 > n_{p+1} > 0$,

c. *if* $p + 1 \neq 1 + n_1$ *then* $n_{p+2} = \cdots = n_{1+n_1} = 1$,

(iii) $n_l = 0$ *for* $l > 1 + n_1$.

Proof of Proposition: First we note that if $N \in \mathcal{N}_0(k)$ achieves $\max\limits_{N \in \mathcal{N}_0(k)} S'(N)$ and $n_1 = k$ then,

(i) $n_0 = n_1 = k$,

(ii) $n_2 = \cdots = n_{k+1} = 1$,

(iii) $n_j = 0$ for $j > k + 1$,

and $S'(N) = 3k^2$.

Now suppose that $n_1 \neq k$ and that $N \in \mathcal{N}_0(k)$ achieves $\max\limits_{N \in \mathcal{N}_0(k)} S'(N)$. We now show this is impossible in a series of cases by appealing to Lemma 4.3.19 which gives the form that N must take and then producing another element of $\mathcal{N}_0(k)$ yielding a greater value of S'.

We need the following equality. From properties (2) and (4) we see that if $n_{p+1} \neq 0$, then

$$n_0 + n_1 + \cdots + n_{2k} = 3k$$

$$k + pn_1 + n_{p+1} + 1 + n_1 - (p + 1) = 3k$$

$$k + (p+1)n_1 + n_{p+1} - p = 3k$$

$$(p+1)n_1 = 2k + p - n_{p+1}$$

$$n_1 = \frac{2k + p - n_{p+1}}{p+1}$$

and that if $n_{p+1} = 0$,

$$n_0 + n_1 + \cdots + n_{2k} = 3k$$

$$k + pn_1 = 3k$$

$$n_1 = \frac{2k}{p}.$$

Let $h = \begin{cases} n_{p+1}, & \text{if } 2 \leq n_{p+1} < n_1; \\ n_1, & \text{if } n_{p+1} < 2. \end{cases}$

We consider the cases: $h = 2$, $h \neq 2$.

Case 1. $h = 2$. Suppose that $h = 2, N \in \mathcal{N}_0(k)$ achieves $\max\limits_{N \in \mathcal{N}_0(k)} S'(N), n_1 \neq k$ and n_1 is as large as possible. If $p = 1$ then $n_1 = \frac{2k-1}{2}$, a contradiction since n_1 is an integer. Thus $p \geq 2$. Let $N' = \langle k, n_1 + 1, \cdots, n_p - 1, 1, \cdots, n_{1+n_1} = 1, 1, 0, \cdots, 0\rangle$. Then $N' \in \mathcal{N}_0(k)$ and $S'(N') = S'(N)$, a contradiction.

At this point, we remark on our peculiar use of notation. The sequence of symbols – $n_p - 1, 1, \cdots, n_{1+n_1} = 1, 1$ – in the $2k+1$-tuple $\langle k, n_1 + 1, \cdots, n_p - 1, 1, \cdots, n_{1+n_1} = 1, 1, 0, \cdots, 0\rangle$, indicates that $n_{p+1} = \cdots = n_{1+n_1} = n_{2+n_1} = 1$.

Case 2. $h \neq 2$. Suppose $h \neq 2, N \in \mathcal{N}_0(k)$ achieves $\max\limits_{N \in \mathcal{N}_0(k)} S'(N)$ and that $h = 2j + 1$.

Let $N' = \begin{cases} \langle k, n_1 + j, \cdots, n_{p+1} = 1, 1, \cdots, n_{1+n_1+j} = 1, 0, \cdots, 0 \rangle, & \text{if } h = n_{p+1}, \\ \langle k, n_1 + j, \cdots, n_p = 1, 1, \cdots, n_{1+n_1+j} = 1, 0, \cdots, 0 \rangle, & \text{if } h = n_1. \end{cases}$

We wish to show that $N' \in \mathcal{N}_0(k)$, and $S'(N') \geq S'(N)$. By considering the terms in the sum S' that change, to check that $S'(N') \geq S'(N)$ we see we need to check

(i)
$$(n_1 + j)^2 + j + 1 \geq {n_1}^2 + (2j + 1)^2,$$

and to ensure that $N' \in \mathcal{N}_0(k)$, all we need to check is

(ii)
$$k - n_1 \geq j.$$

We check *(i)* first and see

$$(n_1 + j)^2 + j + 1 \geq {n_1}^2 + (2j + 1)^2$$

$${n_1}^2 + 2n_1 j + j^2 + j + 1 \geq {n_1}^2 + 4j^2 + 4j + 1$$

$$2n_1 j \geq 3j^2 + 3j$$

$$n_1 \geq \frac{3j + 3}{2}$$

Since $n_1 \geq h$, it is sufficient to check $h = 2j + 1 \geq \frac{3j+3}{2}$. But this inequality is equivalent to $j \geq 1$ or $h \geq 3$, which is clearly true.

We remark at this stage, that the proofs of the succeeding cases will follow the same style. That is, we will start with the inequality that we wish to prove, and reduce it by a sequence of reversible steps to a trivially true inequality. This approach, though somewhat unconventional, makes the proofs, in my opinion, easier to follow.

We now check $k - n_1 \geq j$. Note that if $n_1 \leq \frac{2}{3}k$, then $k - n_1 \geq \frac{1}{3}k \geq \frac{1}{2}n_1 \geq \frac{1}{2}h \geq j$. Thus, we need only to check the cases $p = 1, p = 2$.

Suppose $p = 1$. Then $h \neq n_1$, since this would imply $n_1 = k$. Thus we may suppose $h = n_{p+1}$. We note $j = \frac{h-1}{2}$ and check,

$$k - n_1 \geq j$$

$$k - \left[\frac{2k - h + 1}{2}\right] \geq \frac{h-1}{2}$$

$$\frac{h-1}{2} \geq \frac{h-1}{2}.$$

Suppose $p = 2$ and $h = n_{p+1}$. We check

$$k - n_1 \geq j$$

$$k - \left[\frac{2k - h + 2}{3}\right] \geq \frac{h-1}{2}$$

$$\frac{k + h - 2}{3} \geq \frac{h-1}{2}$$

$$2k + 2h - 4 \geq 3h - 3$$

$$2k \geq h + 1$$

which is clearly true.

Suppose $p = 2$ and $h = n_1$. Then either $n_{p+1} = 0$ or $n_{p+1} = 1$. If $n_{p+1} = 0$, then from (3) we get $n_0 + n_1 + n_2 = k + 2n_1 = 3k$. Hence $n_1 = k$, a contradiction. Thus $n_{p+1} = 1$. We apply (3) again and get

$$n_0 + n_1 + \cdots + n_{2k} = k + n_1 + n_1 + (n_1 + 1) - 2 = 3k \implies n_1 = \frac{2k+1}{3}.$$

Also

$$h = 2j + 1 \implies j = \frac{h-1}{3}.$$

We now check

$$k - n_1 \geq j$$

$$k - \left[\frac{2k+1}{3}\right] \geq \frac{h-1}{3}$$

$$\frac{k-1}{3} \geq \frac{h-1}{3}.$$

This is clearly true.

Now, let us suppose that $h = 2j, h \neq 2$ and $N \in \mathcal{N}_0(k)$ achieves $\max\limits_{N \in \mathcal{N}_0(k)} S'(N)$. Let us suppose further that $h = n_{p+1}$. Let

$$N' = (k, n_1 + j - 1, \cdots, n_{p+1} = 2, 1, \cdots, n_{1+n_1+j-1} = 1, 0, \cdots, 0).$$

We wish to show that $N' \in \mathcal{N}_0(k)$ and that $S'(N') > S'(N)$. Again to verify $S'(N') > S'(N)$ we only need to consider the terms of S' that change. Thus we check

(i) $$(n_1 + (j-1))^2 + 2^2 + (j-1) \geq {n_1}^2 + (2j)^2.$$

Also to verify $N' \in \mathcal{N}_0(k)$, we need to check

(ii) $$k - n_1 \geq j - 1.$$

We check *(i)* first.

$$(n_1 + (j-1))^2 + 2^2 + (j-1) \geq {n_1}^2 + (2j)^2$$

$${n_1}^2 + 2n_1(j-1) + (j-1)^2 + 4 + j - 1 \geq {n_1}^2 + 4j^2$$

$$2n_1(j-1) \geq 4j^2 - (j-1)^2 - 4 - (j-1)$$

$$2n_1(j-1) \geq 4j^2 - j^2 + 2j - 1 - 4 - j + 1$$

$$2n_1(j-1) \geq 3j^2 + j - 4 = (3j+4)(j-1)$$

$$n_1 \geq \frac{3j+4}{2}$$

Since $h \neq n_1, n_1 \geq h+1$. Hence, we check $h + 1 = 2j + 1 \geq \frac{3j+4}{2}$ and obtain $j \geq 2$ or $h \geq 4$ which is clearly true.

As before, to verify *(ii)* we need only consider the cases: $p = 1, p = 2$.

Suppose $p = 1$. We note that $j - 1 = \frac{h-1}{2}$ and check

$$k - n_1 \geq j - 1$$

$$k - \left[\frac{2k-h+1}{2}\right] \geq \frac{h-2}{2}$$

$$\frac{h-1}{2} \geq \frac{h-2}{2}.$$

Suppose $p = 2$. We check

$$k - n_1 \geq j - 1$$

$$k - \left[\frac{2k-h+2}{3}\right] \geq \frac{h-2}{2}$$

$$\frac{k+h-2}{3} \geq \frac{h-2}{2}$$

$$2k + 2h - 4 \geq 3h - 6$$

$$2k \geq h - 2.$$

This is clearly true.

Now let us suppose that $h \neq n_{p+1}$. Let

$$N' = (k, n_1 + j - 1, n_1 + 1, \cdots, n_p = 1, 1, \cdots, n_{1+n_1+j-1} = 1, 0, \cdots, 0).$$

To verify $S'(N') > S'(N)$ we need to check

(i) $$(n_1 + (j-1))^2 + (n_1+1)^2 + 1 + (j-1) \geq 2{n_1}^2.$$

And to verify $N' \in \mathcal{N}_0(k)$ we need to check

(ii) $$k - n_1 \geq j - 1 \text{ and } p \geq 2.$$

We now check *(i)*.

$$(n_1 + (j-1))^2 + (n_1+1)^2 + 1 + (j-1) \geq 2{n_1}^2$$

$${n_1}^2 + 2n_1(j-1) + (j-1)^2 + {n_1}^2 + 2n_1 + 1 + 1 + j - 1 \geq 2{n_1}^2$$

$$j(2n_1 + (j-1)) + 2 \geq 0.$$

This is clearly true.

As before we know that if $p > 2$, then *(ii)* follows. We now show that the cases $p = 1$ and $p = 2$ are impossible. Since $h = n_1$, either $n_{p+1} = 0$ or $n_{p+1} = 1$.

Suppose $p = 1$. Then $n_{p+1} \neq 0$, for if it were 0, then from (3) we would have $k + n_1 = 3k$ or $n_1 = 2k$, a contradiction. Thus, we can assume that $n_{p+1} = 1$. But from the equality $n_1 = \frac{2k+p-n_{p+1}}{p+1}$ we get $n_1 = k$. A contradiction. Thus, we can suppose that $p \geq 2$.

Suppose $p = 2$. If $n_{p+1} = 1$, we have $n_1 = \frac{2k+1}{3}$. But this is impossible as n_1 is an even integer and $\frac{2k+1}{3}$, if it is an integer, is odd. On the other hand, if $n_{p+1} = 0$, then we get $n_1 = \frac{2k}{2} = k$. A contradiction.

Hence, the maximum value of S' over $\mathcal{N}_0(k)$ is $3k^2$. □

Thus we have the following proposition.

Proposition 4.3.20. *The maximum value of S' over $\mathcal{N}$ is $3k^2$ and is achieved by $N = \langle n_0, n_1, \cdots, n_{2k} \rangle$ where*

(i) $n_0 = n_1 = k$,

(ii) $n_2 = \cdots = n_{k+1} = 1$,

(iii) $n_l = 0$ *for* $l > k+1$.

Proposition 4.3.21. *The maximum value of S over all difference families is $3\binom{k}{2}$ and is attained by*

$$V = \{(j, 2k+1-j, 2k+j, 4k+1-j) : 1 \leq j \leq k\}.$$

Proof: First note that each quadruple in V has a sum of both 0 and $2k+1$. Also, each has a sum of $2k+2j = 2(k+j)$ and as 2 is a unit modulo $4k+1$, these values are distinct. Thus, V has the required distribution. Calculating S we see

$$\begin{aligned} S &= \frac{1}{2}(n_0(n_0-1) + ({n_0}^2 + {n_1}^2 + \cdots + {n_{2k}}^2 - 3k) \\ &= \frac{1}{2}(k(k-1) + k^2 + k^2 + \underbrace{1 + \cdots + 1}_{k \text{ times}} - 3k) \\ &= \frac{3k^2 - 3k}{2} \\ &= 3\binom{k}{2}. \end{aligned}$$

□

We now give a lower bound on the minimum degree of G. The proof of this proposition is similar to the proof on the maximum degree of G. Consequently, we will only give a sketch of the proof.

Proposition 4.3.22. *Let m denote the minimum degree of the label graph with parameter k. Then $m \geq k - 1$.*

Sketch of Proof: First we note that if $N \in \mathcal{N}$ minimizes S', then N must have the form

(i) $n_0 = 1$,

(ii) $n_1 = \cdots = n_{k-1} = 2$,

(iii) $n_k = \cdots = n_{2k} = 1$.

Evaluating S for this N we obtain,

$$\begin{aligned} S &= \frac{1}{2}(n_0(n_0 - 1) + (n_0{}^2 + n_1{}^2 + \cdots + n_{2k}{}^2 - 3k) \\ &= \frac{1}{2}(1(1-1) + \underbrace{2^2 + \cdots + 2^2}_{k-1 \text{ times}} + \underbrace{1^2 + \cdots + 1^2}_{k+1 \text{ times}} - 3k) \\ &= \frac{1}{2}(4(k-1) + (k+1) - 3k) \\ &= \frac{1}{2}(2k-3) \\ &= k - \frac{3}{2}. \end{aligned}$$

Thus $m \geq k - 1$. □

Unfortunately, in the case of the minimum degree we can not specify a vertex having minimal degree for each value of k. However, computer experiments indicate that vertices of minimal degree are abundant.

4. Outline of the algorithm

In this section we present a brief synopsis of the preceeding algorithm. Here we assume that a stopping time, MAX, has been determined.

```
*Step 1* Initialize $v$.

        Set $v = \{(j, 2k+1-j, 2k+j, 4k+1-j) : 1 \le j \le k\}$.

*Step 2* Determine the number of switches for $v$: $S(v)$.

        Determine the distribution of sums: $N(v) = (n_0, n_1, \cdots, n_{2k})$.
        Set $S(v) = 2\binom{n_0}{2} + \left[\binom{n_1}{2} + \cdots + \binom{n_{2k}}{2}\right]$.

*Step 3* Determine the number of steps to exit $v$: $E(v)$.

        Set $p = n_0$.
        Choose $r$ uniformly in $[0,1]$.
        Set $E(v) = \left\lfloor \log r \Big/ \log\left(1 - \frac{S(v)+2}{2 \cdot 3^p \left[3\binom{k}{2} + 2\right]}\right)\right\rfloor + 1$.

*Step 4* Increment the iteration counter.

        Set $C = C + E(v)$.

*Step 5* **IF** $C \ge$ MAX **THEN**

        Choose a random difference family represented by the label $v$;
        **STOP**.

    **ELSE**

        Choose $R$ at random from $\{1, 2, \cdots, S(v)+2\}$;
        Determine switch to make;
            **IF** $R = 1$ **THEN** set $v$ to the lexicographically previous vertex,
            **IF** $R = 2$ **THEN** set $v$ to the lexicographically next vertex,
            **IF** $R > 2$ **THEN** make the lexicographically $(R-2)$–nd switch;
        **GOTO** *Step 2*.
```

BIBLIOGRAPHY

[Ald1] D. Aldous, *Some inequalities for reversible Markov chains*, Journal of the London Mathematical Society **25** (1982), no. 2, pp. 564 – 576.

[Ald2] D. Aldous, *Bibliography: Random Walks on Graphs*, (available from author).

[Ald3] D. Aldous, *An introduction to covering problems for random walks on graphs*, Journal of Theoretical Probability **2** (1989), no. 1, pp. 87 – 89.

[Ald4] D. Aldous, *Lower bounds for cover times for reversible Markov chains and random walks on graphs*, Journal of Theoretical Probability **2** (1989), no. 1, pp. 91 – 100.

[Alo] N. Alon, *Eigenvalues and expanders*, Combinatorica **6** (1986), no. 2, pp. 83 – 96.

[Bil] P. Billingsley, *Probability and Measure*, Second Edition, John Wiley and Sons, New York, 1986.

[BlHa] A. Blass and F. Harary, *Properties of almost all graphs and complexes*, Journal of Graph Theory **3** (1979), pp. 225 – 240.

[Bo1] B. Bollobás, *Graph Theory*, Springer-Verlag, New York, 1979.

[Bo2] B. Bollobás, *Random Graphs*, Academic Press, Orlando, 1985.

[Bo3] B. Bollobás (ed.), *Probabilistic Combinatorics and Its Applications*, Proceedings of Symposia in Applied Mathematics; v.44. AMS Short Course lecture notes, American Mathematical Association, Providence, R.I., 1992.

[Br1] N. Brand, *Almost all Steinhaus graphs have diameter two*, Journal of Graph Theory **16** (1992), pp. 213 – 219.

[BCDJ] N. Brand, S. Curran, S. Das and T. Jacob, *Probability of diameter two for Steinhaus graphs*, Discrete Applied Mathematics **41** (1993), pp. 165 – 171.

[BrHu] N. Brand and C. Huffman, *Invariants and constructions of Mendelsohn designs*, Geometriae Dedicata **22** (1987), pp. 173 – 196.

[BrJa] N. Brand and S. Jackson, *Properties of classes of random graphs* (preprint).

[BrMo] N. Brand and M. Morton, *Generalized Steinhaus graphs* (preprint).

[BrDu] R. Brigham and R. Dutton, *Distances and diameters in Steinhaus graphs*, Congressus Numerantium **76** (1990), pp. 7 – 14.

[BrWi1] G. Brightwell and P. Winkler, *Extremal cover times for random walks on trees*, Journal of Graph Theory **14** (1990), no. 5, pp. 545 – 554.

[BrWi2] G. Brightwell and P. Winkler, *Maximum hitting times for random walks on graphs*, Random Structures and Algorithms **1** (1990), no. 3, pp. 263 – 276.

[Br2] A. Broder, *How hard is it to marry at random? (On the approximation of the permanent.)*, Proceedings of the 18th ACM Symposium on the Theory of Computing (1986), pp. 50 – 58.

[Br3] A. Broder, *Errata to "How hard is it to marry at random? (On the approximation of the permanent)"*, Proceedings of the 20th ACM Symposium on the Theory of Computing (1988), p. 551.

[BrKa] A. Broder and A. Karlin, *Bounds on the cover time*, Journal of Theoretical Probability **2** (1989), no. 1, pp. 101 – 120.

[BrSh] A. Broder and E. Shamir, *On the second eigenvalue of random regular graphs*, (Preliminary version), Proceedings of the 28th Symposium on the Foundations of Computer Science (1987), pp. 286 – 294.

[Ch1] K. Chung, *Markov Chains with Stationary Transition Probabilities*, Springer-Verlag, New York, 1967.

[CGW] F. Chung, R. Graham and R. Wilson, *Quasi-random graphs*, Combinatorica **9** (1989), pp. 345 – 362.

[Dey] A. Dey, *Theory of Block Designs*, Wiley Eastern Limited, New Delhi, 1986.

[DoSn] P. Doyle and J.L. Snell, *Random Walks and Electric Networks*, Carus Mathematical Monograph; no. 22, Mathematical Association of America, U.S.A., 1984.

[DyFr] M. Dyer and A. Frieze, *Computing the volume of convex bodies: a case where randomness provably helps*, in Probabilistic Combinatorics and Its Applications (B. Bollobás, ed.), Proceedings of Symposia in Applied Mathematics; v.44. AMS Short Course lecture notes, American Mathematical Association, Providence, R.I., 1992, pp. 123 – 169.

[ErRe1] P. Erdős and A. Rényi, *On random graphs I.*, in Paul Erdős: The Art of

Counting, Selected Writings (J. Spencer, ed.), The MIT Press, Cambridge, 1973, pp. 561 - 568.

[ErRe2] P. Erdős and A. Rényi, *On the evolution of random graphs*, in Paul Erdős: The Art of Counting, Selected Writings (J. Spencer, ed.), The MIT Press, Cambridge, 1973, pp. 574 - 617.

[Fe] W. Feller, *An Introduction to Probability Theory and Its Application, Volume I*, Third Edition, John Wiley and Sons, New York, 1968.

[GeWo] P. Gerl and W. Woess, *Simple random walks on trees*, European Journal of Combinatorics **7** (1986), pp. 321 - 331.

[GrSt] G. Grimmett and D. Stirzaker, *Probability and Random Processes*, Second Edition, Oxford University Press, New York, 1992.

[GöJa] F. Göbel and A.A. Jagers, *Random walks on graphs*, Stochastic Processes and their Applications **2** (1974), pp. 311 - 336.

[Ha] M. Hall, *Combinatorial Theory*, Second Edition, John Wiley and Sons, New York, 1986.

[JeSi] M. Jerrum and A. Sinclair, *Conductance and the rapid mixing property for Markov chains: the Approximation of the permanent resolved*, (Preliminary version), Proceedings of the 20th ACM Symposium on the Theory of Computing (1988), pp. 235 - 244.

[JeSi2] M. Jerrum and A. Sinclair, *Approximating the permanent*, SIAM Journal of Computation **18** (1989), no. 6, pp. 1149 - 1178.

[JeSi3] M. Jerrum and A. Sinclair, *Fast uniform generation of regular graphs*, Theoretical Computer Science **73** (1990), pp. 91 - 100.

[Jo] P. John, *Incomplete Block Designs*, Lecture notes in statistics; v. 1, Marcel Dekker, New York, 1980.

[KSK] J. Kemeny, J. Snell and A. Knapp, *Denumerable Markov Chains*, Springer-Verlag, New York, 1976.

[KLNS] J. Kahn, N. Linial, N. Nisan and M. Saks, *On the cover time of random walks on graphs*, Journal of Theoretical Probability **2** (1989), no. 1, pp. 121 - 128.

[Ku] V. Kulkarni, *Generating random combinatorial objects*, Journal of Algorithms **11** (1990), pp. 185 - 207.

[Lu] T. Luczak, *On the equivalence of two basic models of random graphs*, in Random Graphs '87 (M. Karoński, J Jaworski and A. Ruciński, eds.), John Wiley and Sons, New York, 1990, pp. 151 - 157.

[Ma] P. Matthews, *Some sample path properties of a random walk*, Journal of Theoretical Probability **2** (1989), no. 1, pp. 129 - 146.

[Mi] M. Mihail, *Conductance and convergence of Markov chains - a combinatorial treatment of expanders -*, (Extended abstract), 30th Annual Symposium on Foundations of Computer Science (1989), pp. 526 - 531.

[Mo1] J. Moon, *Random walks on random trees*, Journal of the Australian Mathematical Society **15** (1973), pp. 42 - 53.

[Mo2] J. Moon, *Various proofs of Cayley's formula for counting trees*, in A Seminar on Graph Theory (F. Harary, ed.), Holt, New York, 1967, pp. 70 - 78.

[Pa] E. Palmer, *Graphical Evolution*, John Wiley and Sons, New York, 1985.

[Ro1] S. Ross, *Introduction to Probability Models*, Fourth Edition, Academic Press, San Diego, 1989.

[Ro2] S. Ross, *Stochastic Processes*, John Wiley and Sons, New York, 1983.

[Ry] H. Ryser, *Combinatorial Mathematics*, Carus Mathematical Monograph; no. 14, Mathematical Association of America, U.S.A., 1963.

[Si] A. Sinclair, *Algorithms for Random Generation and Counting*, Birkhäuser, Boston, 1993.

[SiJe] A. Sinclair and M. Jerrum, *Approximate counting, uniform generation and rapidly mixing Markov chains*, Information and Computation **82** (1989), pp. 93 - 133.

[Va] U. Vazirani, *Rapidly mixing Markov chains*, in Probabilistic Combinatorics and Its Applications (B. Bollobás, ed.), Proceedings of Symposia in Applied Mathematics; v.44. AMS Short Course lecture notes, American Mathematical Association, Providence, R.I., 1992, pp. 99 - 121.

[Wi] H. Wilf, *Combinatorial Algorithms: An Update*, S.I.A.M., Philadelphia, 1989.

[Zu] D. Zuckerman, *Covering times of random walks on bounded degree trees and other graphs*, Journal of Theoretical Probability **2** (1989), no. 1, pp. 147 – 157.